~~Bibliographic patent files

18/3,K/3 (Item 3 from file: 350)
DIALOG(R)File 350:Derwent WPIX

0013067249 - Drawing available
WPI ACC NO: 2003-147219/200314
Related WPI Acc No: 2003-711858
XRPX Acc No: N2003-116218
Object securing method in cryptographic data securing system, involves adding object which is encrypted using working split formed by combining
splits including random key components, with header
Patent Assignee: TECSEC INC (TECS-N)
Inventor: DOMANGUE E L; SCHEIDT E M
Patent Family (1 patents, 1 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update
US 6490680	B1	20021203	US 199768785	P	19971204	200314 B
			US 1998205221	A	19981204	

Priority Applications (no., kind, date): US 199768785 P 19971204; US 1998205221 A 19981204

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
US 6490680	B1	EN	17	6	Related to Provisional US 199768785

Class Codes
International Classification (Main): **H04L-009/00**
(Additional/Secondary): **H04L-009/30**

Original Publication Data by Authority

Original Abstracts:
A process of encrypting an object includes applying a **hash** algorithm to the **object** , generating a random number, combining a first plurality of splits including the random number to...

...the hashed object according to a selected algorithm using the working split as a key, **forming** a header **including information** that can be used to decrypt the object, encrypting the header, and adding the encrypted
...
Claims:
What is claimed is: 1. A process of securing an object, comprising: applying a cryptographic **hash** algorithm to the object to provide a **hash** **value** ; storing the **hash** value on a token; **generating** a random key component; combining **a** first plurality of key components to form a first

key; encrypting the object using the...

...of key components to form a second key; encrypting the random key component using the **second** key to form an encrypted key component; encrypting the **hash** value according to a digital signature algorithm using a user **private** **key** , to provide a digital signature; encrypting
the **hash** value according **to** a user algorithm using the first key; **forming** a header including **information** that can be used to decrypt the
encrypted object, **wherein** the information includes the user algorithm,
the encrypted key component, and decrypt read credentials; encrypting...

18/3,K/5 (Item 5 from file: 350)
DIALOG(R)File 350:Derwent WPIX

0012315417 - Drawing available
WPI ACC NO: 2002-256981/200230
XRPX Acc No: N2002-198955
**Member information registration method for on-line store, involves matching
and storing individual identifiers and verification code received from terminal device and mobile telephone**
Patent Assignee: FURUHATA T (FURU-I); GOUNOHARA S (GOUN-I); SAITOU A (SAIT-I); SONY COMPUTER ENTERTAINMENT INC (SONY); SONY COMPUTER ENTERTAINMENT KK (SONY)
Inventor: FURUHATA T; FURUHATA T S C E I; GONOHARA S; GOUNOHARA S; GOUNOHARA S S C E I; SAITO A; SAITOU A
Patent Family (11 patents, 33 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
WO 2001097060	A2	20011220	WO 2001JP5166	A	20010618	200230	B
AU 200164306	A	20011224	AU 200164306	A	20010618	200231	E
BR 200106748	A	20020416	BR 20016748	A	20010618	200234	E
			WO 2001JP5166	A	20010618		
JP 2002074188	A	20020315	JP 2001177151	A	20010612	200234	E
US 20020087543	A1	20020704	US 2001882369	A	20010615	200247	E
KR 2002026258	A	20020406	KR 2002702037	A	20020216	200267	E
EP 1290572	A2	20030312	EP 2001938716	A	20010618	200320	E
			WO 2001JP5166	A	20010618		
CN 1401104	A	20030305	CN 2001802094	A	20010618	200338	E
MX 2002001639	A1	20020801	WO 2001JP5166	A	20010618	200367	E
			MX 20021639	A	20020215		
TW 564358	A	20031201	TW 2001114634	A	20010615	200431	E
US 6789078	B2	20040907	US 2001882369	A	20010615	200459	E

Priority Applications (no., kind, date): JP 2000177151 A 20010612; JP 2000181651 A 20000616; JP 2001177151 A 20010612

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
WO 2001097060	A2	EN	40	4	

National Designated States,Original: AU BR CA CN IN KR MX NZ RU SG

Regional Designated States,Original: AT BE CH CY DE DK ES FI FR GB GR IE
IT LU MC NL PT SE TR
AU 200164306 A EN Based on OPI patent WO 2001097060
BR 200106748 A PT PCT Application WO 2001JP5166
Based on OPI patent WO 2001097060
JP 2002074188 A JA 12
EP 1290572 A2 EN PCT Application WO 2001JP5166
Based on OPI patent WO 2001097060
Regional Designated States,Original: AT BE CH CY DE DK ES FI FR GB GR IE
IT LI LU MC NL PT SE TR
MX 2002001639 A1 ES PCT Application WO 2001JP5166
Based on OPI patent WO 2001097060
TW 564358 A ZH

Original Titles:
...PROCEDE ET SYSTEME D'ENREGISTREMENT D'INFORMATIONS RELATIVES A **DES** MEMBRES, ET PROCEDE ET SYSTEME DE VERIFICATION DESDITS MEMBRES...

...PROCEDE ET SYSTEME D'ENREGISTREMENT D'INFORMATIONS RELATIVES A **DES** MEMBRES, ET PROCEDE ET SYSTEME DE VERIFICATION DESDITS MEMBRES

Original Publication Data by Authority

Original Abstracts:
...are inputted to web server for mobile telephones 12, web server
for mobile telephones 12 **extracts identification information**
specific to the mobile telephone 12 and records it linked to the already-registered member...
Claims:
...to a second device outputted from the second device, extracting from the
member database member **data matching** both the received **individual identifier** and verification code, **adding** the identification information
specific to the second device to the extracted member data, and updating...

18/3,K/6 (Item 6 from file: 350)
DIALOG(R)File 350:Derwent WPIX

0011209033 - Drawing available
WPI ACC NO: 2002-147820/200219
XRPX Acc No: N2002-112048
Electronic data processing in which data key is produced by combining **a**
secret key **with a random number**
Patent Assignee: GEMPLUS (GEMP-N); GEMPLUS SCA (GEMP-N); GUTERMAN P (GUTE-I)
Inventor: GUTERMAN P
Patent Family (6 patents, 93 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
WO 2001099335	A1	20011227	WO 2001FR1942	A	20010620	200219	B
FR 2810480	A1	20011221	FR 20007887	A	20000620	200219	E
AU 200169215	A	20020102	AU 200169215	A	20010620	200230	E
EP 1297653	A1	20030402	EP 2001947556	A	20010620	200325	E
			WO 2001FR1942	A	20010620		
US 20030179884	A1	20030925	WO 2001FR1942	A	20010620	200364	E
			US 2002311693	A	20021219		
CN 1437808	A	20030820	CN 2001811332	A	20010620	200374	E

Priority Applications (no., kind, date): FR 20007887 A 20000620

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
WO 2001099335	A1	FR	26	4	

National Designated States,Original: AE AG AL AM AT AU AZ BA BB BG BR BY
BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN
IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ
PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
Regional Designated States,Original: AT BE CH CY DE DK EA ES FI FR GB GH
GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW

AU 200169215	A	EN	Based on OPI patent WO 2001099335
EP 1297653	A1	FR	PCT Application WO 2001FR1942
			Based on OPI patent WO 2001099335

Regional Designated States,Original: AL AT BE CH CY DE DK ES FI FR GB GR
IE IT LI LT LU LV MC MK NL PT RO SE SI TR.

US 20030179884	A1	EN	PCT Application WO 2001FR1942

Electronic data processing in which data key is produced by combining **a**
secret key **with a random number**

Class Codes
International Classification (Main): **H04L-009/00** ...
... **H04L-009/08** ...

... **H04L-009/14**
... (Additional/Secondary): **H04L-009/20**

Original Publication Data by Authority

Original Abstracts:
...stored number (R1) are applied (E3) as inverse (F1-1) of the function
(F1) to **produce** a third key (K3) used **for** processing the **data** , properly speaking. The device can be a smart card and the data the confidential code...

...stored number (R1) are applied (E3) as inverse (F1 -1) of

the function (F1) **to** produce a third key (K3) used for **processing**
the data, properly speaking. The device can be a smart card and the data
the confidential...

...inverse (F1-1) de la fonction (F1) pour produire une troisieme cle (K3)
servant au **traitement** des donnees proprement dit. Le dispositif peut etre
une carte a puce et les donnees

18/3,K/10 (Item 10 from file: 350)
DIALOG(R)File 350:Derwent WPIX

0010766720 - Drawing available
WPI ACC NO: 2001-380826/200140
XRPX Acc No: N2001-279239
Generation method for shared secret value between entities, involves computing common shared key for each entity by combining group short term public key, intra-entity shared key, and entity long term key
Patent Assignee: CERTICOM CORP (CERT-N); VANSTONE S A (VANS-I)
Inventor: VANSTONE S A
Patent Family (8 patents, 90 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
WO 2001006697	A2	20010125	WO 2000CA838	A	20000719	200140	B
AU 200061437	A	20010205	AU 200061437	A	20000719	200140	E
CA 2277633	A1	20010119	CA 2277633	A	19990719	200140	E
EP 1226678	A2	20020731	EP 2000947716	A	20000719	200257	E
			WO 2000CA838	A	20000719		
EP 1226678	B1	20031022	EP 2000947716	A	20000719	200373	E
			WO 2000CA838	A	20000719		
DE 60006147	E	20031127	DE 60006147	A	20000719	200403	E
			EP 2000947716	A	20000719		
			WO 2000CA838	A	20000719		
US 6934392	B1	20050823	US 2000619633	A	20000719	200556	E
US 20060123235	A1	20060608	US 2000619633	A	20000719	200639	E
			US 2005155899	A	20050620		

Priority Applications (no., kind, date): CA 2277633 A 19990719

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
WO 2001006697	A2	EN	11	2	

National Designated States,Original: AE AL AM AT AU AZ BA BB BG BR BY CA
CH CN CR CU CZ DE DK DM EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE
KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU
SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
Regional Designated States,Original: AT BE CH CY DE DK EA ES FI FR GB GH

GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TZ UG ZW
AU 200061437 A EN Based on OPI patent WO 2001006697
CA 2277633 A1 EN
EP 1226678 A2 EN PCT Application WO 2000CA838
Based on OPI patent WO 2001006697
Regional Designated States,Original: AL AT BE CH CY DE DK ES FI FR GB GR
IE IT LI LT LU LV MC MK NL PT RO SE SI
EP 1226678 B1 EN PCT Application WO 2000CA838
Based on OPI patent WO 2001006697
Regional Designated States,Original: CH DE FR GB LI
DE 60006147 E DE Application EP 2000947716
PCT Application WO 2000CA838
Based on OPI patent EP 1226678
Based on OPI patent WO 2001006697
US 20060123235 A1 EN Continuation of application US 2000619633
Continuation of patent US 6934392

Alerting Abstract DESCRIPTION - An entity long term **private key** and a corresponding entity long term public key for each entity by **combining** the long term private and public keys of each members of the entity. A short...

...of each member. The intra-entity public key is computed for each member by mathematically **combining** its short-term **private key** , the long term **private key** and the intra-entity shared key...

Class Codes
International Classification (Main): **H04L-009/00** ...

... **H04L-009/30**
International Classification (+ Attributes)
IPC + Level Value Position Status Version
H04L-0009/00 ...

Original Publication Data by Authority

Original Abstracts:
...each member then computing an intra-entity shared key by mathematically combining the short term **keys** of each of the members computing an intra-entity public key by mathematically **combining** its short-term **private key** , the long **term private key** and the **intra - entity** shared key. Next, each entity **combines** intra-entity public **keys** to derive a group short-term Si public key; each entity transmitting its intra-entity...

...term public keys of each the members computing an intra-entity public key by mathematically **combining** its short-term private key, the long term private **key** and the intra-entity shared key. Next, each entity

combines
intra-entity public keys to derive a group **short** -term Si public **key**
;
each entity transmitting its **intra** - **entity** shared key and its group
short term public key **to** the other entities; and each entity
computing a
common shared key K by combining its...

...members within an entity. For each member then computing an intra-
entity
shared key by **mathematically** **combining** the short term public keys
of
each the members computing an intra-entity public key by mathematically
combining its short-term **private** **key** , the long term **private** **key**
and the intra-entity shared key. Next, each entity **combines** intra-
entity
public keys to derive a group short-term Si public key; each entity...

...entity shared key and its group short term public key to the other
entities; and **each** entity computing a **comm**on shared key K by
combining **its** group short term public key (Si), with the intra-
entity
shared key (Xi), and a group short term public (Si) key received
from...

...of the members; exchanging short term public keys of the members
within
an entity. For **each** member then computing an intra-entity shared **key**
by mathematically combining the short term keys of each of the members
computing an intra-entity public key by mathematically **combining** its
short-term **private** **key** , **the** **long** term **private** **key** and the
intra-entity shared key. Next, each entity **combines** intra-entity
public
keys to derive a group short-term S...key to the other entities; and
each
entity computing a common shared key K by **combining** its group short
term
public key (Si), with the intra-entity shared key (Xi), **and** a group
short
term **public** (Si) key **received** **from** the other entitites.
...

...L'invention concerne un procede permettant de creer une valeur
secrete
partagee entre **des** entites dans un systeme de communications de
donnees,
au moins une de ces entites ayant...

...a creer une cle privee et une cle publique correspondante de courte
duree pour chacun **des** membres; et a echanger les cles publiques de
courte
duree **des** membres au sein d'une entite. Pour chaque membre, on
calcule
alors une cle partagee...

...cles publiques de courte duree de chaque membre et une cle publique
intra-entite en **combinant** mathematiquement sa cle privee de courte

duree,
la cle privee de longue duree et la...

...entite transmet, a d'autres entites, sa cle partagee intra-entite et sa
cle publique **de** groupe de courte duree. Chaque entite calcule enfin une
cle **partagee** commune K en combinant sa cle publique de groupe de courte
duree (Si) avec la...

...partagee intra-entite (Xi) et une cle publique de groupe de courte duree
(Si) provenant **des** autres entites.
Claims:
...term public key said method comprising the steps of:(a) generating an
entity long term **private** **key** and corresponding entity long term public
key for each entity by **combining** the long term private and **public keys**
of each members of the entity.(b) generating a short term private and a
corresponding short term public key for each **of** **the** members;(c)
exchanging short term public keys of the members within **an** entity;(d) for
each member:(iii) computing an intra-entity shared key by mathematically
combining...

...public keys of each said member;(iv) computing an intra-entity public
key by mathematically **combining** its short-term **private** **key** , the long
term **private** **key** and said intra-entity shared key;(e) for each entity
combining intra-entity public keys to derive a group short- **term** public
key;(f) each entity transmitting its intra-entity shared key and its group
short term public key to said **other** entities; and(g) **each** **entity**
computing a common **shared** **key** K by **combining** its group short term
public key, with the intra-entity shared **key** , and an entity an entity
long term public key received from the other entity...

...privee a court terme et d'une cle publique a court terme correspondante
pour chacun **des** membres;(c) echange **des** cles publiques a court terme
des membres a l'interieur d'une entite;(d) pour chaque membre:(iii) calcul
d'une...

...cle privee a court terme, la cle privee a long terme et ladite cle
partagee **intra** -entite;(e) pour chaque entite **combinaison** **des** cles
publiques intra-entite **pour** deriver une cle publique a court terme de
groupe;(f) chaque entite transmettant sa cle...

...long terme d'entite recue de l'autre entite.

...term public key said method comprising the steps of:(a) generating an entity long term **private key** and corresponding entity long term public key for each entity by **combining** the long term private and public keys of each members of the entity.(b) generating...

...an entity;(d) for each member:i. computing an intra-entity shared key by mathematically **combining** said short term public keys of each said member;ii. computing an intra-entity public key by mathematically **combining** its short-term **private key** , the long term **private key** and said intra-entity shared key;(e) **for each** entity **combining** intra-entity public keys to derive a group short- **term** public key;(f) each entity transmitting its intra-entity shared key and its group short...
... 1. A **method** for **generating** a shared secret **value** between entities (A, B) in **a data** communication system, one or more of said entities having a plurality of members (Ai, Bi) for participation in said communication system, each member having a long term **private key** and a corresponding long term **public** key said method comprising the steps of:(a) generating an entity long term public key...

...public keys of each said member;ii. computing an intra-entity public key by mathematically **combining** its short-term **private key** , the long term **private key** and said intra-entity shared key;(e) for each entity **combining** intra-entity public keys to derive a group short-term public key;(f) **each entity** making its intra-entity shared key and its entity long term public key available to

18/3,K/13 (Item 13 from file: 350)
DIALOG(R)File 350:Derwent WPIX

0009666487 - Drawing available
WPI ACC NO: 1999-620008/199953
XRPX Acc No: N1999-457288
Public key generating method for secure digital communication system
Patent Assignee: CERTICOM CORP (CERT-N); QU M (QUMM-I); VANSTONE S A (VANS-I)
Inventor: QU M; VANSTONE A; VANSTONE S A
Patent Family (13 patents, 82 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
WO 1999049612	A1	19990930	WO 1999CA244	A	19990323	199953	B
CA 2232936	A1	19990923	CA 2232936	A	19980323	200008	E

CA 2235359	A1	19990923	CA 2235359	A	19980420	200008	E
AU 199928235	A	19991018	AU 199928235	A	19990323	200009	E
EP 1066699	A1	20010110	EP 1999908723	A	19990323	200103	E
			WO 1999CA244	A	19990323		
JP 2002508529	W	20020319	WO 1999CA244	A	19990323	200222	E
			JP 2000538463	A	19990323		
AU 758044	B	20030313	AU 199928235	A	19990323	200328	E
EP 1066699	B1	20040721	EP 1999908723	A	19990323	200449	E
			WO 1999CA244	A	19990323		
DE 69918818	E	20040826	DE 69918818	A	19990323	200456	E
			EP 1999908723	A	19990323		
			WO 1999CA244	A	19990323		
US 6792530	B1	20040914	WO 1999CA244	A	19990323	200460	E
			US 2000667819	A	20000922		
US 20050114651	A1	20050526	WO 1999CA244	A	19990323	200535	E
			US 2000667817	A	20000922		
			US 2004921870	A	20040820		
DE 69918818	T2	20050825	DE 69918818	A	19990323	200560	E
			EP 1999908723	A	19990323		
			WO 1999CA244	A	19990323		
IL 138660	A	20060221	IL 138660	A	19990323	200634	E

Priority Applications (no., kind, date): CA 2232936 A 19980323; CA 2235359 A 19980420

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
WO 1999049612	A1	EN	45	2	

National Designated States,Original: AL AM AT AU AZ BA BB BG BR BY CA CH
CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IS JP KE KG KP KR KZ
LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK
SL TJ TM TR TT UA UG US UZ VN YU ZW

Regional Designated States,Original: AT BE CH CY DE DK EA ES FI FR GB GH
GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ UG ZW

CA 2232936	A1	EN		
CA 2235359	A1	EN		
AU 199928235	A	EN		Based on OPI patent WO 1999049612
EP 1066699	A1	EN		PCT Application WO 1999CA244
				Based on OPI patent WO 1999049612

Regional Designated States,Original: CH DE FR GB LI

JP 2002508529	W	JA	90	PCT Application WO 1999CA244
				Based on OPI patent WO 1999049612
AU 758044	B	EN		Previously issued patent AU 9928235
				Based on OPI patent WO 1999049612
EP 1066699	B1	EN		PCT Application WO 1999CA244
				Based on OPI patent WO 1999049612

Regional Designated States,Original: CH DE FR GB LI

DE 69918818	E	DE		Application EP 1999908723
				PCT Application WO 1999CA244
				Based on OPI patent EP 1066699
				Based on OPI patent WO 1999049612

US 6792530	B1	EN	Continuation of application WO 1999CA244
US 20050114651	A1	EN	Continuation of application WO 1999CA244
			Continuation of application US 2000667817
			Continuation of patent US 6334747
DE 69918818	T2	DE	Application EP 1999908723
			PCT Application WO 1999CA244
			Based on OPI patent EP 1066699
			Based on OPI patent WO 1999049612
IL 138660	A	EN	Based on OPI patent WO 1999049612

Class Codes
...International Classification (Main): **H04L-009/00** ...

... **H04L-009/08** ...

... **H04L-009/30**
(Additional/Secondary): **H04L-009/32**

Original Publication Data by Authority

Original Abstracts:
...the implicit certificate information (IA, gammaA) in accordance with a
mathematical function F(gammaA, IA) **to** derive an entity information f;
generating a **private key** (a) of the entity A by signing the entity information f and transmitting the private...

...the trusted entity selects a unique identity distinguishing the entity
A. The trusted entity then **generates** a public **key** reconstruction public
data of the entity A by mathematically combining public values obtained
from respective private values of...

...values of the trusted entity. The trusted entity transmits the value kA
to the entity **to** permit A to generate a **private key** from kA, A's private value and A's **implicit** certificate. The entity A's public **key**
information may be reconstructed from public information, and A's implicit
certificate...

...entity then generates a public key reconstruction public data of the entity A by mathematically combining public values obtained from respective **private values** of the trusted entity and the entity A. The
unique identity and public key reconstruction...
...entity transmits the value kA to the entity A to permit A to generate a
private key from kA, A's private value and A' **s** implicit certificate.

The entity A's public **key information may** be reconstructed from public information, **and** A's implicit certificate...

...A method of **generating a** public key in a secure digital communication system, having at least one trusted entity CA...

...key (a) of the entity A by signing the entity information f and transmitting the **private key** (a) to the entity A,whereby the **entity**
A's public key may be reconstructed from the public information, the generator gammaA and ...publique dans un systeme de communication numerique
sur ayant au moins une entite CA et **des** entites d'abonnes A. Ce procede
consiste a faire en sorte que, pour chaque entite A, la CA selectionne une
entite unique IA distinguant l'entite A; a generer **des** donnees publiques
de reconstruction de la cle publique gammaA d'entite A par la combinaison
...

...une information d'entite f;a generer une cle privee a de l'entite A **en**
signant l'information d'entite f et en transmettant la cle privee a a l'entite A, la cle publique de l'entite A pouvant etre reconstruite a partir **des** informations publiques, **du** generateur gammaA et de l'identite IA de maniere relativement efficace. Selon une autre variante,
un certificat de cle publ
Claims:
...ist;b) die das Vertrauen geniessende Entitat CA erzeugt ein offentliches
Datum gammaA zur Rekonstruktion **des** offentlichen Schlussels einer Entitat
A durch mathematische Kombination offentlicher Werte, die **aus** jeweiligen
geheimen Werten der das Vertrauen geniessenden Entitat CA und der Entitat A
erhalten wurden...

...durch Verknupfen der besagten Entitatsinformation mit geheimen Werten
der das Vertrauen geniessenden Entitat CA,Ubertragen **des** besagten Wertes
kA zu der Entitat A, um es A zu ermoglichen, einen geheimen Schlussel...

...und dem impliziten Zertifikat zu erzeugen, wobei der offentliche Schlussel der Entitat A aus offentlicher **Information** , dem besagten offentlichen Datum gammaA zur Rekonstruktion **des** offentlichen Schlussels
und der besagten Identitat IA rekonstruiert werden kann...

... A method of generating a...

...d) generating a value kA by binding said entity information f with

private values of **said** trusted entity CA.transmitting said value kA to
said entity A to permit A to generate a **private key** from said value kA,
the private value of said entity A, and said implicit certificate, whereby
said entity **A** 's public key may be reconstructed from public information,
said public key reconstruction public data...

...un systeme de communication numerique securise (10), comportant au moins
une entite fiable CA et **des** entites d'abonnes A, ledit procede comprenant
les etapes dans lesquelles / de:a) pour chaque...

...selectionne une identite unique IA distinguant ladite entite A;b) ladite
entite fiable CA genere **des** donnees publiques de reconstruction de cle
publique gammaA d'une entite A en combinant mathematiquement les valeurs
publiques obtenues a partir **des** valeurs privees respectives de ladite
entite fiable CA et de ladite entite A, pour obtenir...

...F(IA, gammaA) pour deduire une information d'entite f,d) generer une
valeur KA **en** liant ladite information d'entite f aux valeurs privees de
ladite entite fiable CA,transmettant...

...une cle privee a partir de ladite valeur KA, la valeur privee de ladite
entite **A** , et ledit certificat implicite, moyennant quoi ladite cle
publique de l'entite A peut etre reconstruite a partir d'une information
publique, desdites donnees **publiques** de reconstruction de cle publique yA
et de ladite identite IA.

~~Full text patent files

18/3,K/4 (Item 4 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01977623
Method and system for protecting individual information
Verfahren und System zum Schutz von individuellen Informationen
Procede et systeme pour protection d'informations individuelles
PATENT ASSIGNEE:
SONY CORPORATION, (214024), 7-35, Kitashinagawa 6-chome Shinagawa-ku,
Tokyo, (JP), (Applicant designated States: all)
INVENTOR:
Hamano, Atsushi Sony Corporation, 7-35, Kitashinagawa 6-chome
Shinagawa-ku, Tokyo, (JP)

Shinozaki, Ikuo Sony Corporation, 7-35, Kitashinagawa 6-chome
Shinagawa-ku, Tokyo, (JP)
LEGAL REPRESENTATIVE:
Korber, Martin Hans et al (88321), Mitscherlich & Partner Patentanwalte
Sonnenstrasse 33, 80331 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1594029 A2 051109 (Basic)
APPLICATION (CC, No, Date): EP 2005009353 050428;
PRIORITY (CC, No, Date): JP 2004136419 040430
DESIGNATED STATES: AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES; FI; FR; GB; GR;
HU; IE; IS; IT; LI; LT; LU; MC; NL; PL; PT; RO; SE; SI; SK; TR
EXTENDED DESIGNATED STATES: AL; BA; HR; LV; MK; YU
INTERNATIONAL PATENT CLASS (V7): G06F-001/00
ABSTRACT WORD COUNT: 65
NOTE:
Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200545	1914
SPEC A	(English)	200545	11924
Total word count - document A			13838
Total word count - document B			0
Total word count - documents A + B			13838

...SPECIFICATION 1), "(parallel to)" means combining.
Namely, the signature/encoding circuit 55 encodes a result of **combining** the verification data of boot program VBP and **hash** data P3P-**hash** by the private **key** **data** Kpri-sc1 to **generate** data VF.
The signature/encoding circuit 55 writes the generated data VF in the memory...

...3), "(parallel to)" indicates combining.
Namely, the signature/encoding circuit 55 encodes a result of **combining** the verification data of boot program VBP, **hash** data P3P-**hash** and privacy policy data by using POL and private **key** **data** Kpri-sc1 to **generate** data VF1.
The signature/encoding circuit 55 writes the generated data VF1 to the memory...

18/3,K/9 (Item 9 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01310513
Optical disk with copy protection, method for manufacturing and method for reading such a disk
Optische Platte, Verfahren zur Herstellung und Verfahren zum Lesen

einer
solchen Platte
Disque optique, procede pour fabriquer et proceder pour lire un tel disque
PATENT ASSIGNEE:
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD., (1855503), 1006, Oaza Kadoma,
Kadoma-shi, Osaka 571, (JP), (Proprietor designated states: all)
INVENTOR:
Oshima, Mitsuaki, 115-3, Minamitatsumi-cho, Katsura, Nishikyo-ku,
Kyoto-shi, Kyoto 615, (JP)
Gotoh, Yoshiho, Room 201, 9-17, Higashinakahama 4-chome, Jyoto-ku,
Osaka-shi, Osaka 536, (JP)
LEGAL REPRESENTATIVE:
Grunecker, Kinkeldey, Stockmair & Schwanhausser Anwaltssozietat (100721)
, Maximilianstrasse 58, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1120777 A2 010801 (Basic)
EP 1120777 A3 011010
EP 1120777 B1 050126
APPLICATION (CC, No, Date): EP 2001108949 951116;
PRIORITY (CC, No, Date): JP 94283415 941117; JP 9516153 950202; JP 95261247
951009
DESIGNATED STATES: DE; FR; GB
RELATED PARENT NUMBER(S) - PN (AN):
EP 741382 (EP 95938017)
RELATED DIVISIONAL NUMBER(S) - PN (AN):
EP 1480204 (EP 2004020082)
INTERNATIONAL PATENT CLASS (V7): G11B-020/00; G06F-001/00; G11B-007/00; G11B-027/30; G11B-023/28; G11B-013/04; G11B-011/105; G11B-019/02; G11B-019/12; G11B-007/007; G11B-007/26; G11B-020/12; G11B-027/10
ABSTRACT WORD COUNT: 37
NOTE:
Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200131	207
CLAIMS B	(English)	200504	294
CLAIMS B	(German)	200504	298
CLAIMS B	(French)	200504	360
SPEC A	(English)	200131	21556
SPEC B	(English)	200504	21209
Total word count - document A			21766
Total word count - document B			22161
Total word count - documents A + B			43927

...SPECIFICATION on software locked or unlocked at their option.
This in turn means that pirates cannot **produce** pirated disks unless
they steal the sub **secret** **key** **information** unique to the software
from the software maker.
In Figure 32, the software maker **combines** disk physical position

information 868 and disk ID 869, and encrypts them together by using the
sub **secret key** 876 in step 866f to construct a public key **cipher** 859 which is recorded on the optical disk 800 in the form of a barcode...

...SPECIFICATION on software locked or unlocked at their option.
This in turn means that pirates cannot **produce** pirated disks unless
they steal the sub **secret key information** unique to the software
from the software maker.
In Figure 32, the software maker **combines** disk physical position information 868 and disk ID 869, and encrypts them together by using the
sub **secret key** 876 in step 866f to construct a public key **cipher** 859 which is recorded on the optical disk 800 in the form of a barcode...

18/3,K/11 (Item 11 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00641946
A METHOD AND APPARATUS FOR GENERATING A CIPHER STREAM
VERFAHREN UND EINRICHTUNG ZUR ERZEUGUNG EINER CHIFFRIERSEQUENZ
PROCEDE ET APPAREIL POUR GENERER UNE SUITE DE DONNEES CHIFFREE
PATENT ASSIGNEE:
TELSTRA CORPORATION LIMITED, (1157613), A.C.N. 051 775 556, 242 Exhibition Street, Melbourne, VIC 3000, (AU), (Proprietor designated states: all)
INVENTOR:
TAYLOR, Richard, 29 Sherbrooke Lodge Road, Sherbrooke, VIC 3789, (AU)
LEGAL REPRESENTATIVE:
Cross, Rupert Edward Blount et al (42891), BOULT WADE TENNANT, Verulam Gardens 70 Gray's Inn Road, London WC1X 8BT, (GB)
PATENT (CC, No, Kind, Date): EP 681768 A1 951115 (Basic)
EP 681768 A1 980204
EP 681768 B1 010328
WO 9416509 940721
APPLICATION (CC, No, Date): EP 94903705 931230; WO 93AU687 931230
PRIORITY (CC, No, Date): AU 92PL6577 921230
DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
INTERNATIONAL PATENT CLASS (V7): **H04L-009/26**
NOTE:
No A-document published by EPO
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	200113	1058
CLAIMS B	(German)	200113	888

CLAIMS B (French) 200113 1249
SPEC B (English) 200113 5152
Total word count - document A 0
Total word count - document B 8347
Total word count - documents A + B 8347

INTERNATIONAL PATENT CLASS (V7): **H04L-009/26**

...SPECIFICATION sequence zj)) which comprises the cipher stream. The basis
of operation of the cipher stream **generator** 2 is that **secret key data** xam)) is provided to the stream **cipher** 2, which **combines** the
linear pseudo random data sequences produced by LFSR's 8, performs a non-linear transformation thereon, and a **cipher** stream is output at 14,
for combination with a message to be enciphered. The terminal receiving
the enciphered message is also provided with a **cipher** stream generator
2, such that a transformation involving the **cipher** stream zj)) and the
enciphered message can be utilised to decipher the message. Equations (1
...

18/3,K/13 (Item 13 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2007 WIPO/Thomson. All rts. reserv.

00989323 **Image available**
A SECURE ACCESS METHOD AND SYSTEM
PROCEDE ET SYSTEME D'ACCES SECURISE
Patent Applicant/Assignee:
DATAPLAY INC, 2560 55th Street, Boulder, CO 80301-5706, US, US (Residence), US (Nationality)
Inventor(s):
FELDMAN Timothy R, 1029 Grant Avenue, Louisville, CO 80027, US,
LEE Lane W, 894 S. Bermont Drive, Lafayette, CO 80026, US,
BRAITBERG Michael F, 440 Broken Fence Road, Boulder, CO 80302, US,
RAYBURN Douglas M, 1200 Galapago Street, Apt. 318, Denver, CO 80204, US,
KIWIMAGI Gary G, 17427 West County Road 18E, Loveland, CO 80537, US,
VOLK Steven B, 3805 Norwood Court, Boulder, CO 80304, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200319334 A2-A3 20030306 (WO 0319334)
Application: WO 2002US27303 20020826 (PCT/WO US0227303)
Priority Application: US 2001940083 20010827; US 2001940174 20010827; US
2001940025 20010827; US 2001940035 20010827; US 2001940026 20010827; US
2001939896 20010827; US 2001939960 20010827
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM

DZ
EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR
LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI
SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 30213

Fulltext Availability:
Detailed Description

Detailed Description
... public key. In block 3224, CKU Server 2860 decrypts the Session Key
using a Server **Private Key** . In block 3226, CKU Server 2860 decrypts
Key Complements, for example, using PKI with a Server **Private Key** and
add Session **Key information** . In block 3228, CKU Server 2860
generates a random key using, for example, **AES** and/or triple- **DES** to
be used to re-encrypt the Key Complements that provide unlock capability.
Block 3230...

...the CKU Server 2860 encrypts the Key Complements using the Unlock Key,
using, for example, **AES** and/or triple- **DES** . In block 3232, CKU Server
2860 encrypts the Unlock Key using the engine public key...

18/3,K/16 (Item 16 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00483529
CRYPTOGRAPHIC CO-PROCESSOR
COPROCESSEUR CRYPTOGRAPHIQUE
Patent Applicant/Assignee:
INFORMATION RESOURCE ENGINEERING INC,
KAPLAN Michael M,
DOUD Robert Walker,
KAVSAN Bronislav,
OBER Timothy,
REED Peter,
Inventor(s):
KAPLAN Michael M,
DOUD Robert Walker,
KAVSAN Bronislav,

OBER Timothy,
REED Peter,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9914881 A2 19990325
Application: WO 98US19316 19980916 (PCT/WO US9819316)
Priority Application: US 9759082 19970916; US 9759839 19970916; US 9759840 19970916; US 9759841 19970916; US 9759842 19970916; US 9759843 19970916; US 9759844 19970916; US 9759845 19970916; US 9759846 19970916 ; US 9759847 19970916
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH GM
HR HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX
NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZW GH
GM KE LS MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES

FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML MR NE SN
TD TG
Publication Language: English
Fulltext Word Count: 95649

Main International Patent Class (v7): **H04L-009/06**
Fulltext Availability:
Detailed Description

Detailed Description
... Key storage may be expanded to 700 Secret Keys by assigning segments
of the ADSP2183 **internal** Data RAM to be 'Protected'. This is accomplished via a CGX LWT command argument.
Encrypt...IC)
* 16-bit CRC of the Laser Data
The Program Control Data (PCD) bits include **configuration** for permitted
Key
Lengths, Algorithm Enables, Red KEK loading, Internal IC Pulse Shaping
Characteristics, etc. Some of the...OxOOO3 Diffie-Hellman public kev, key
exchange.

Table 19 Puhlic Key Algorithm Definitions
One-Way **Hash** Algorithms
The following table defines the supported one way **HASH** algorithms and
their operating modes. The constant values referenced in the table must
be used to access the CGX Kernel's one-way **HASH** algorithms.

170
NN ame Value Msg. Digest Length Description
CGX **MD5** A 0x0000 128 bits (16 bytes) Specifies the **MD5** one way **HASH**
algorithm.

CGX SHS A 0x000 1 160 bits (20 bytes) Specifies NIST's one way **HASH**
algorithm, SHS
Table 20 One Way IMSH Algorithm Definitions
IPsec Symmetric Key Transformation Algorithms
The...user keys to be uncovered using any of
the supported secret key algorithms (i.e., **DES** , Triple **DES** , etc.), in
any of the modes (i.e., ECB, CFB, OFB, and CBC). As for GKEKs,
they can only be uncovered by the LSV in the triple **DES** CBC mode;
any attempt to bypass this will fail. The operation copies the secret key
...

...the GKEK, any key to be
uncovered by a GKEK must also use the triple **DES** CBC mode. Also,
an IV will be returned in the application supplied IV buffer of...

...requirement is that the parent
KEK (i.e. LSV) to GKEKs must be a triple **DES** key and the GKEK
176
itself must be a triple **DES** key. This implies the use of triple **DES**
in
the CBC mode when these two KEKs are used for uncovering and
covering of...key cache
register, destkey, in the RED form.

The Generate KEK command only generates Triple- **DES** secret
keys. Once a GY.EK is created, the secure Kernel only recognizes the
GKEK...

...GKEK, the application is not allowed to specify any algorithm; the
secure Kernel assumes triple **DES** in CBC mode. Also, the application
is not allowed to provide a IV;, the secure...

...Command Name: CGX
GEN
RKEK
Command Description.

An RKEK is a Diffie-Hellman negotiated, triple **DES** , trusted
symmetrical key. The RKEK is created by an application, an escrow
agent and IPLE...

...key cache
register, destkey, in the RED form.

The Generate RKEK command only generates Triple- **DES**
secret keys. Once an RKEK is created, the secure Kernel only
recognizes the RKEK as...
...RKEY, the application is not allowed to specify any

algorithm, the secure Kernel assumes triple **DES** in CBC mode. Also, the application is not allowed to provide a IV;, the secure... VPTR)destkey-, 185 /* type of secret key to generate, use one of the following.

CGX- **DES** X and CGX-TREPLE- **DES** -A kb->cb->arguxnent[1] = (VPTR)key type; /* length of user secret key to generate...an application's pass-phrase. The secret key is derived by taking the one-way HASH of the application's pass phrase and using the message digest for it as the...

...newly generated key is not a KEK), not the LSV.

The application can choose the **HASH** algorithm to be used via the argument, **hash** -alg. Furthermore, the algorithm for choosing which bits to use is outlined in Nficrosoft's...

...the algorithm only supports key bit lengths between 32 bits and 112 bits when creating **DES** or Triple **DES** keys, 32 bits through 160 bits when creating I-MUC keys, and 32 bits through...kemelblock *kb, unsigned short pswd pg, unsigned short *pswd, unsigned short pswd -len, unsigned short **hash** , Og, kcr destkey, unsigned short key jype, unsigned short length, unsigned short use, secretkey *bk...

...the application's pass phrase string in bytes kb->cb->argument[I1 = (VPTR)pswdlen; /* the **HASH** aIg to use: CGX-SHS A, or CGX- **MD5** -A kb->cb->argument[2] = (VPfR) **hash** alg; /* KCR ID number to place newly generated user secret key kb->cb->argument[3] = (VPTR)destkey-, /* type of secret key to generate, use one of the following.

CGX- **DES** A, and CGX-TRIPLE- **DES** -A kb->cb->argument[4] = (VPTR)key type; /* length of user secret key to generate...

...transforms on an existing secret key. The transform command allows the application to create the **HMAC** , CBC **DES** , or CBC

Triple **DES** keys. Furthermore, it can be used to create the IV and replay
counters and beyond...

...key, this command places a copy of the
key in its RED form (if an **HMAC** or CBC **DES** key is to be generated) in
a
KCR location and returns a BLACK copy of...
...However, the application can change the key type to any valid supported
key (i.e. **DES** , triple **DES** , or RC5) via the ...passed in as a NULL
pointer, the operation will return a message digest via the **hash**
-context object argument, hc. This returned **hash** context may be red or
black (covered.) If the caller wishes the returned **hash** context to be
black, the user must specify a crypto context, hkek, which the command
will use to cover the returned **hash** context, hc. If the user supplies a
NULL parameter for hkek, hc will be returned...

...as specified by the argument, klen. If the key to transform is to be a
DES key and klen is less then or equal to 7 bytes, then 64 bytes of...

~~Bibliographic NPL files

**********of interest**********
21/3,K/2 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC

06768051 INSPEC Abstract Number: B9801-6120B-045, C9801-6130S-033
Title: Cryptographic key recovery
Author(s): Al-Salqan, Y.Y.
Author Affiliation: Sun Microsyst. Inc., Palo Alto, CA, USA
Conference Title: Proceedings of the Sixth IEEE Computer Society Workshop
on Future Trends of Distributed Computing Systems (Cat. No.97TB100190) p.34-7
Publisher: IEEE Comput. Soc, Los Alamitos, CA, USA
Publication Date: 1997 Country of Publication: USA xii+346 pp.
ISBN: 0 8186 8153 5 Material Identity Number: XX97-02929
U.S. Copyright Clearance Center Code: 1071-0485/97/$10.00
Conference Title: Proceedings of the Sixth IEEE Computer Society Workshop
on Future Trends of Distributed Computing Systems
Conference Sponsor: IEEE Comput. Soc. Tech. Committee on Distributed
Process
Conference Date: 29-31 Oct. 1997 Conference Location: Tunis,

Tunisia
Language: English
Subfile: B C

...Abstract: encrypted data. The mechanism does not require keys to be escrowed. It is based on **adding** an extra small field-the Key Recovery Entry (KRE)-to a message or file being transmitted. This mechanism facilitates key recovery both for session keys in symmetric cryptographic systems and **private keys** in asymmetric cryptographic systems without any need to escrow any key information. The author makes...
...Identifiers: **private keys** ;

21/3,K/4 (Item 4 from file: 2)
DIALOG(R)File 2:INSPEC

06496176 INSPEC Abstract Number: B9703-6120B-118, C9703-6130S-056
Title: Non-repudiation without public-key
Author(s): Taylor, R.
Author Affiliation: Defence Sci. & Technol. Organ., Jamieson, ACT, Australia
Conference Title: Information Security and Privacy. First Australasian Conference, ACISP'96. Proceedings p.27-37
Editor(s): Pieprzyk, J.; Seberry, J.
Publisher: Springer-Verlag, Berlin, Germany
Publication Date: 1996 Country of Publication: Germany ix+331 pp.
ISBN: 3 540 61991 7 Material Identity Number: XX96-03585
Conference Title: Information Security and Privacy. First Australasian Conference, ACISP'96. Proceedings
Conference Sponsor: Australasian Soc. Electron. Security; Univ. Wollongong
Conference Date: 24-26 June 1996 Conference Location: Wollongong, NSW, Australia
Language: English
Subfile: B C

...Abstract: By dropping the unconditional security property a related scheme with less memory storage requirements is **constructed** . In relation to the options for providing non-repudiation some discussion of the complexity of the cryptanalysis of public and **private key** cryptosystems is provided.

...Identifiers: **private** **key** cryptosystems

**********of interest**********

21/3,K/7 (Item 1 from file: 35)

01164497 ORDER NO: AAD91-19534

ON THE KEY INFORMATION REDUNDANCY IN SECRET - KEY **CRYPTOSYSTEMS (CRYPTOSYSTEMS,** CIPHER **SYSTEMS)**

Author: YANG, JOHNSON CHUNG-HUANG

Degree: PH.D.
Year: 1990
Corporate Source/Institution: UNIVERSITY OF SOUTHWESTERN LOUISIANA (0233
)
Source: VOLUME 52/02-B OF DISSERTATION ABSTRACTS INTERNATIONAL.
PAGE 999. 108 PAGES

ON THE KEY INFORMATION REDUNDANCY IN SECRET - KEY **CRYPTOSYSTEMS (CRYPTOSYSTEMS,** CIPHER **SYSTEMS)**

...information redundancy in stream ciphers. The improved linear syndrome method is developed to attack sequence **generators** in which an enciphered sequence is correlated to a sequence produced by an LFSR with known feedback polynomial. The method is applied to crack the Beth-Piper stop-and-go **generator** and Geffe's **generator** .

The linear consistency test is **derived** based on the estimation of the consistency probability of a system of linear algebraic equations...

...The method developed was applied to discover the key information redundancy in the Jennings multiplexing **generator** and the Massey-Rueppel multi-speed **generator** .

A new class of keystream **generator** is **constructed** on the basis of mutual clock control of two LFSRs. The sequence produced by the new scheme has a large non-Mersenne prime period of the **form** $q \cdot 2\sp{n} -$ 1 and a linear complexity comparable with the period. A new primality test is also **derived** .

The cryptanalytic strength of the Hwang-Rao Secret Error-Correcting Code (SECC) schemes are examined...

~~Full text NPL files - 1

19/3,K/2

07479223 (USE FORMAT 7 OR 9 FOR FULLTEXT)

Sonera, Gemplus and EDS Launch Global Initiative To Promote Secure Mobile Commerce

PR NEWSWIRE
September 28, 1999
JOURNAL CODE: WPRW LANGUAGE: English RECORD TYPE: FULLTEXT
WORD COUNT: 1269

(USE FORMAT 7 OR 9 FOR FULLTEXT)

... and decrypting a message. Traditional cryptography has usually involved the creation and sharing of a **secret key** for the encryption and decryption of messages. Using of asymmetric encryption methods requires reliable distribution...

... authorities and reliable third parties, which offer services. The objective of the infrastructure is to **produce** reliable security service for the net.

In the Public Key Infrastructure, physical identification takes place only once when key information - public and **secret key** - is tied to party's user identity. The public key and its certificate are publicly...

... encryption method is used, the length of the key or the safe place of the **secret key** . In the Public Key Infrastructure, the authorities in certain countries aim to define national responsibilities...

...and Private Key Cryptography Works

In public key cryptography, a public and private key are **created** simultaneously using the same algorithm (a popular one is known as RSA) by a certificate authority (CA). The **private key** is given only to the requesting party and the public key is **made** publicly available (as part of a digital certificate) in a directory that all parties can access. The **private key** is never shared with anyone or sent across the Internet. You use the **private key** to decrypt text that has been encrypted with your public key by someone else (who...

...I send you a message, I can find out your public key (but not

your
private key) from a central administrator and encrypt a message to you
using your public key. When you receive it, you decrypt it with your
private key . In addition to encrypting messages (which ensures
privacy), you can authenticate yourself to me (so I know that it is really
you who sent the message) by using your **private key** to encrypt a
digital certificate. When I receive it, I can use your public key...

~~Full text NPL files - 2

22/3,K/1 (Item 1 from file: 9)
DIALOG(R)File 9:Business & Industry(R)
(c) 2007 The Gale Group. All rts. reserv.

00864754 Supplier Number: 23399840 (USE FORMAT 7 OR 9 FOR FULLTEXT)
S-A UNVEILS SECURITY SYSTEM
(Scientific-Atlanta Inc has unveiled its digital set-top security system)
Multichannel News, v 18, n 3, p 45+
January 15, 1996
DOCUMENT TYPE: Journal ISSN: 0276-8593 (United States)
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 1146

(USE FORMAT 7 OR 9 FOR FULLTEXT)

TEXT:
...Corp. and RSA are supporting the new system as well.

The new Terisa public key/ **private key**0 system **combines** the security in
the transport layer offered by Netscape's system, which is designed to...

22/3,K/3 (Item 2 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2007 ProQuest Info&Learning. All rts. reserv.

01663108 03-14098
Protecting digital media content
Memon, Nasir; Wong, Ping Wah
Communications of the ACM v41n7 PP: 34-43 Jul 1998
ISSN: 0001-0782 JRNL CODE: ACM
WORD COUNT: 4301

...TEXT: s watermarking algorithm was extended to a public-key scheme in
which a user's **private key** is needed to insert the watermark, as in
Figure 3. However, watermark **extraction** requires only the public key.

The
LSB of each pixel in a block is stripped...

...size parameters are hashed and the result encrypted using a public-key
algorithm. The resulting **cipher** text and the binary watermark image are
combined using an exclusiveOR function; the result is then embedded into
the LSB of the block. In the **extraction** step, the same MSB data and the
image size parameters are hashed. The LSB of the data block (**cipher** text)
is decrypted using a corresponding public key decryption algorithm. The
decrypted result and the **hash** output are **combined** using an exclusive-OR
function to **produce** the visual watermark. The public-key extension
certainly expands the practical applicability of this watermarking...

22/3,K/6 (Item 2 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

01747641 Supplier Number: 42189170 (USE FORMAT 7 FOR FULLTEXT)
ADDRESSING SECURITY
Network Computing, p57
July, 1991
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 1555

... are secret, be secure. An example of such an algorithm is the Data
Encryption Standard (**DES**) developed by the National Institute of
Standards and Technology (NIST). Products based on **DES** are widely
available. What's more, the algorithm is easy to use because it can be
built into encryption programs and then **combined** with a **secret key** to
produce effective encryption.
Encryption systems can be symmetric or asymmetric. In a symmetric
system, the sender...

22/3,K/8 (Item 2 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

04132346 SUPPLIER NUMBER: 07826888 (USE FORMAT 7 OR 9 FOR FULL TEXT)
**Lock up your data. (Software Review) (UltraLock and FastLock data security
programs) (evaluation)**
Kendrick, Nigel
PC User, n117, p105(3)
Oct 11, 1989
DOCUMENT TYPE: evaluation ISSN: 0263-5720 LANGUAGE: ENGLISH

RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 1675 LINE COUNT: 00131

... complex multiuser protection systems with different levels of access and a mix of global and **private keys** . New files cna inherit keys
based upon those previously entered for their home directory.
Installation...

**********of interest**********

22/3,K/11 (Item 3 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2007 The Gale Group. All rts. reserv.

02074073 SUPPLIER NUMBER: 19516596 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Keep your notebook data secure with Session Key. (Secured Communications
Canada Session Key PC Card security device) (Hardware Review) (Evaluation)
Brown, Bruce
Computer Shopper, v17, n7, p246(1)
July, 1997
DOCUMENT TYPE: Evaluation ISSN: 0886-0556 LANGUAGE: English
RECORD TYPE: Fulltext; Abstract
WORD COUNT: 530 LINE COUNT: 00044

...ABSTRACT: key with strong encryption software. The product prevents tampering by using a hardware key to **make** data unreadable to those without the card even if they have the password. Session Key...

...security technologies including passwords, digital signatures and several types of encryption. It supports both the **DES** -ECB and CBC symmetric encryption modes and the RSA, DSA and DH public/ **private** - **key**
algorithms as well as Digest and **Hash** modes. The PC Card manages encryption with an on-board RISC processor and flash memory...

~~Full text NPL files - 3

19/3,K/2 (Item 2 from file: 810)
DIALOG(R)File 810:Business Wire
(c) 1999 Business Wire . All rts. reserv.

0665903 BW0231

SPYRUS MAC: Multi-Card Accelerator from SPYRUS is Hardware Cryptographic
Digital Signature Server Solution; Scaleable, High-Assurance
Certification Authority, Remote Access, and Other Digital Content
Signing Applications Now Enabled

January 27, 1997

Byline: Business Editors and Computer Writers

...security
posture of the supported application system.
"Software-based cryptographic implementations rely on storage of **private key information** within the server host, exposing the **private**

key to attack from both local and network hackers," said Sue Pontius, SPYRUS CEO. "The core...

...on the EES LYNKS Privacy
Card technology. The essential security features of this technology are: **private key generation** in hardware; tamper-resistant and cryptographically protected private key storage; and secure on-card cryptographic...

...and the need
for a secure, scaleable solution for operational deployments. With the MCA, all **private keys** are **generated** and retained within the confines of the tamper-resistant EES LYNKS Privacy Cards. All security...

19/3,K/3 (Item 3 from file: 810)
DIALOG(R)File 810:Business Wire
(c) 1999 Business Wire . All rts. reserv.

0520713 BW1046

ATALLA: Atalla Begins Shipping Hardware-Based Security for the Internet

October 02, 1995

Byline: Business Editors and Computer Writers

...unauthorized access, disclosure, alteration, duplications and substitution. WebSafe supports both public (e.g. RSA) and **secret key** (e.g. **DES**) technology and employs sophisticated key management similar to global EFT/POS payment networks.
WebSafe is...

...and
the Internet operate very differently. For example, the bank payment network primarily relies on **secret keys** (like **DES**) for security, while the Internet typically relies on both secret and public keys (like RSA...

19/3,K/5 (Item 2 from file: 813)
DIALOG(R)File 813:PR Newswire
(c) 1999 PR Newswire Association Inc. All rts. reserv.

0990442 MNTU011
Network Systems Security Devices Tested by Department of Defense-

Sponsored
'SPOCK' Program

DATE: September 3, 1996 12:58 EDT WORD COUNT: 645

... packet-by-packet using the most powerful encryption algorithms
available,
including the Data Encryption Standard (**DES** and Triple **DES**), NSC1 and
the
International Data **Encryption Algorithm** (IDEA). Public/ **private key**
exchange
uses both RSA(TM) algorithms and Diffie-Hellman protocol.

SPOCK conducts test of the...

**********of interest**********

19/3,K/8 (Item 5 from file: 813)
DIALOG(R)File 813:PR Newswire
(c) 1999 PR Newswire Association Inc. All rts. reserv.

0776490 NY011
TELEQUIP CORPORATION INTRODUCES THE CRYPTA PLUS CARD

DATE: January 9, 1995 08:05 EST WORD COUNT: 790

...The Crypta Plus card's CSP provides secure computing functions such as random number generation, **private key** operations and key
comparisons,
while the **private key information** never leaves the secure silicon.
Multiple passwords can be stored on the Crypta Plus card...

19/3,K/14 (Item 2 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext
(c) 2007 CMP Media, LLC. All rts. reserv.

01097494 CMP ACCESSION NUMBER: NWC19960715S0021
Psstt! Security Designed For Your Eyes Only (Security)
Kiran Movva
NETWORK COMPUTING, 1996, n 711, PG54
PUBLICATION DATE: 960715
JOURNAL CODE: NWC LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Sneak Previews
WORD COUNT: 1121

... of the confidential portion of the keys.
Your Eyes Only uses five different types of **secret key** encryption
algorithms: **DES** (56 bits), Triple **DES** (effectively 112 bits), RC4
(

128 bits), RC5 (128 bits) and Blowfish (128 bits)-all of...

...by Your Eyes Only suffices most internal confidentiality needs.
To facilitate the exchange of the **secret key** , Your Eyes Only first encrypts the data with a unique and random **secret key** ; its length depends on the selected **encryption algorithm** . The **secret key** is then encrypted with the receiver's public key. When the data reaches the receiver, the **secret key** is decrypted using the receiver's **private key** , and then the data is decrypted using the **secret key** (see diagram at left). The only caveat is that the recipient must have Your Eyes Only software because there is no standard
for **forming** keys. Your Eyes Only uses its own **format** for its keys just as other products do.
For a 550-KB file, it took...

...additional IDs later. You are also asked to pick the size of your public key/ **private key** pair (The recommended value is 768 bits, but
Your Eyes Only can handle a maximum...

...key sizes slow down the encryption/decryption time. Finally, the setup
process prompts you to **create** an "Unlock" disk, which, in the event you
lose your password, lets you or other...

...the Administrator version. When used by itself, it lets a central coordinator generate public key/ **private key** pairs for users, maintain
passwords, user information and view user audit logs, over the network or
via disks. You can also **generate** setup disks for users with the **key**
information , and a default recipient list (key chain). When used with
Norton Administrator for Networks, you...

19/3,K/22 (Item 5 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

017538
Security is key to ECON
Byline: Ellen Messmer, Washington Correspondent
Journal: Network World Page Number: 64
Publication Date: August 19, 1991
Word Count: 361 Line Count: 26

Text:
... variety of encryption techniques, including RSA Data Security, Inc.'s
public-key encryption algorithms, the **private - key Data** Encryption
Standard and the public-key digital signature **encryption algorithm**

expected to be issued by the National Institute of Standards and
Technology.
Public-key systems...

**********of interest**********

19/3,K/24 (Item 2 from file: 13)
DIALOG(R)File 13:BAMP
(c) 2007 The Gale Group. All rts. reserv.

00505602 Supplier Number: 23623265 (USE FORMAT 7 OR 9 FOR FULLTEXT)
SOMETHING TO TALK ABOUT
(Three organizations are utilizing voice authentication to satisfy various
security needs concerning access control)
Article Author(s): Markowitz, Judith, PhD
Security Management, v 40, n 9, p 58-66
September 1996
DOCUMENT TYPE: Journal ISSN: 0145-9406 (United States)
LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 3842

(USE FORMAT 7 OR 9 FOR FULLTEXT)

TEXT:
...the authorization code to the employee with instructions to call an 800
number, select a **private password** , and enroll by saying the password
three times. The newly **created** voiceprint is stored as a 200-byte pattern.

Preferred retains no password information other than...

19/3,K/26 (Item 2 from file: 56)
DIALOG(R)File 56:Computer and Information Systems Abstracts
(c) 2007 CSA. All rts. reserv.

0000294350 IP ACCESSION NO: 315050
Cryptographic key recovery

Al-Salqan, Yahya Y
Sun Microsystems, Inc, Palo Alto, CA, USA

PAGES: 34-37
PUBLICATION DATE: 1997

PUBLISHER: IEEE COMP SOC, LOS ALAMITOS, CA, (USA)

CONFERENCE:
The 1997 6th IEEE Workshop on Future Trends of Distributed Computing Systems, Tunis, Tunisia, 29-31 Oct. 1997

DOCUMENT TYPE: Conference Paper
RECORD TYPE: Abstract

LANGUAGE: English
FILE SEGMENT: Computer & Information Systems Abstracts

ABSTRACT:
... encrypted data. The mechanism does not require keys to be escrowed. It is based on **adding** an extra, small, field- Key Recovery Entry (KRE) to a message or file being transmitted. This mechanism facilitates key recovery for both session-keys in symmetric cryptographic system, and **private keys** in the asymmetric cryptographic systems without any need to escrow any **key information** . The author makes the differentiation between key escrow and key recovery.

~~Bibliographic patent files

```
? show files;ds
File 347:JAPIO Dec 1976-2007/Mar(Updated 070809)
         (c) 2007 JPO & JAPIO
File 350:Derwent WPIX 1963-2007/UD=200755
         (c) 2007 The Thomson Corporation
File 371:French Patents 1961-2002/BOPI 200209
         (c) 2002 INPI.  All rts. reserv.

Set     Items   Description
S1   14337992   GENERAT??? OR AUTOGENERAT??? OR CONFIGUR? OR
CONSTRUCT??? -
             OR CREAT??? OR DERIV??? OR EXTRACT??? OR FORM??? OR
FORMULAT?-
             ?? OR MADE OR MAKE OR PRODUCE OR PRODUCING OR SYNTHESI?
S2      12732   (KEY OR KEY- OR VARIABLE()VALUE OR
PASSWORD)()(INFORMATION
             OR DATA)
S3    1507163   SUM OR SUMMING OR COMBIN??? OR ADD OR ADDING
S4       7305   (INTERNAL OR PRIVATE OR SECRET OR RESTRICTED OR
LIMITED()A-
             CCESS)()((KEY OR KEYS OR VARIABLE()VALUE OR PASSWORD))
S5       9870   (UNIQUE OR DISTINCTIVE OR INDIVIDUAL OR
DISTINGUISHING)()(-
             ID OR IDENTIFIER OR IDENTIFIERS OR TOKEN OR TOKENS OR TAG
OR -
             TAGS OR INDICATOR OR INDICATORS) OR UI OR UID
S6     954738   DATA()DEVICE OR STORAGE()MEDIUM OR DISK OR DISKS OR
DISC OR
              DISCS OR CD OR DVD OR CDROM OR REMOVABLE()MEMORY OR
(THUMB OR
              USB OR FIREWIRE OR FLASH OR DETACHABLE OR REMOVABLE OR
PORTA-
             BLE OR MEMORY)()(DRIVE OR DRIVES)
S7    2622904   ENCRYPTION()(ALGORITHM  OR FORMULA? ?) OR CIPHER OR DES
OR
             HASH OR MD5 OR AES OR SHA-1 OR SHA()1 OR SHA1 OR HMAC
S8       2949   S1(5N)S2
S9        231   S3(10N)(S4 OR (S5(5N)S6))
S10         0   S7(S)S8(S)S9
S11        12   S7 AND S8 AND S9
S12      3739   S1(10N)S2
S13       320   S3(20N)(S4 OR (S5(10N)S6))
S14         1   S7(S)S12(S)S13
S15        14   S7 AND S12 AND S13 AND IC=(H04K OR H04L)
S16        17   S11 OR S14 OR S15
S17        17   IDPAT (sorted in duplicate/non-duplicate order)
S18        17   IDPAT (primary/non-duplicate records only)
```

18/AN,AZ,TI/1   (Item 1 from file: 350)

DIALOG(R)File 350:(c) 2007 The Thomson Corporation. All rts. reserv.

0015212577

Digital image watermarking apparatus, has watermark generating portion dividing digital image into multiple regions, assigning preset secret keys

to related regions, and generating watermark for each region using related
keys

Original Titles:
VORRICHTUNG UND VERFAHREN ZUM VERSEHEN DIGITALER BILDER MIT WASSERZEICHEN
APPARATUS AND METHOD FOR WATERMARKING DIGITAL IMAGE
DISPOSITIF ET PROCEDE DE TATOUAGE D'IMAGES NUMERIQUES
Apparatus and method for watermarking digital image
APPARATUS AND METHOD FOR WATERMARKING DIGITAL IMAGE
DISPOSITIF ET PROCEDE DE TATOUAGE D'IMAGES NUMERIQUES
Local Applications (No Type Date): US 200547664 A 20050202; WO 2005KR233
A 20050127; KR 20046595 A 20040202; CN 200580000206 A 20050127; EP
2005726294 A 20050127; WO 2005KR233 A 20050127
Priority Applications (no., kind, date): KR 20046595 A 20040202

18/AN,AZ,TI/2 (Item 2 from file: 350)

0013167178
Confidential data transmitting method for a pay television environment uses
shared secret session key system

Original Titles:
Verfahren zur Ubertragung vertraulicher Daten
Verfahren zur Schlusselubereinkunft in einem sicheren Kommunikationssystem
Key agreement method for secure communication system
Methode pour convenir d'une cle pour un systeme de communication securise
Verfahren zur Schlusselubereinkunft in einem sicheren Kommunikationssystem
Key agreement method for secure communication system
Methode pour convenir d'une cle pour un systeme de communication securise
Method of transmitting confidential data
Local Applications (No Type Date): EP 200216814 A 20020726; DE 10137152
A 20010730; US 2002206212 A 20020729; CN 2002127165 A 20020730; KR
200244803 A 20020730; EP 200216814 A 20020726; DE 60208273 A 20020726; EP 200216814 A 20020726; SG 20024502 A 20020724; CN 2002127165 A 20020730; DE 60208273 A 20020726; EP 200216814 A 20020726
Priority Applications (no., kind, date): EP 200216814 A 20020726; DE 10137152 A 20010730

18/AN,AZ,TI/3 (Item 3 from file: 350)

0013067249
Object securing method in cryptographic data securing system, involves adding object which is encrypted using working split formed by combining splits including random key components, with header

Original Titles:
Access control and authorization system
Local Applications (No Type Date): US 199768785 P 19971204; US 1998205221 A 19981204
Priority Applications (no., kind, date): US 199768785 P 19971204; US 1998205221 A 19981204

18/AN,AZ,TI/4 (Item 4 from file: 350)

0012417718
Unique encryption key stream generation apparatus for each data block in a frame during transmission over air interface using session key generated using dynamic system parameters

Original Titles:
METHOD AND APPARATUS FOR GENERATING AN UNIQUE ENCRYPTION KEY STREAM FOR EACH DATA BLOCK IN A FRAME
PROCEDE ET APPAREIL PERMETTANT DE GENERER UN UNIQUE FLOT DE CLES DE CRYPTAGE POUR CHAQUE BLOC DE DONNEES DANS UNE TRAME
Local Applications (No Type Date): WO 2001US25368 A 20010813; AU 200184870 A 20010813
Priority Applications (no., kind, date): US 2000644922 A 20000823

18/AN,AZ,TI/5 (Item 5 from file: 350)

0012315417
Member information registration method for on-line store, involves matching and storing individual identifiers and verification code received from terminal device and mobile telephone

Original Titles:
VERFAHREN UND SYSTEM ZUR AUFZEICHNUNG VON MITGLIEDERDATEN UND VERFAHREN UND
SYSTEM ZUR MITGLIEDERUBERPRUFUNG
MEMBER INFORMATION REGISTRATION METHOD AND SYSTEM,AND MEMBER VERIFICATION
METHOD AND SYSTEM
PROCEDE ET SYSTEME D'ENREGISTREMENT D'INFORMATIONS RELATIVES A **DES** MEMBRES, ET PROCEDE ET SYSTEME DE VERIFICATION DESDITS MEMBRES
METHOD AND DEVICE FOR REGISTERING MEMBER INFORMATION, METHOD AND DEVICE

FOR
CERTIFYING MEMBER AND SERVER COMPUTER
Member information registration method and system, and member verification
method and system
Member information registration method and system, and member verification
method and system
MEMBER INFORMATION REGISTRATION METHOD AND SYSTEM,AND MEMBER VERIFICATION
METHOD AND SYSTEM
PROCEDE ET SYSTEME D'ENREGISTREMENT D'INFORMATIONS RELATIVES A **DES** MEMBRES, ET PROCEDE ET SYSTEME DE VERIFICATION DESDITS MEMBRES
Local Applications (No Type Date): WO 2001JP5166 A 20010618; AU 200164306
A 20010618; BR 20016748 A 20010618; WO 2001JP5166 A 20010618; JP 2001177151 A 20010612; US 2001882369 A 20010615; KR 2002702037 A 20020216; EP 2001938716 A 20010618; WO 2001JP5166 A 20010618; CN 2001802094 A 20010618; WO 2001JP5166 A 20010618; MX 20021639 A 20020215; TW 2001114634 A 20010615; US 2001882369 A 20010615
Priority Applications (no., kind, date): JP 2000177151 A 20010612; JP 2000181651 A 20000616; JP 2001177151 A 20010612

18/AN,AZ,TI/6 (Item 6 from file: 350)

0011209033
Electronic data processing in which data key is produced by combining **a**
secret key **with a random number**

Original Titles:
DATENVERARBEITUNG MITTELS SCHLUSSEL
DATA PROCESSING WITH A KEY
TRAITEMENT DE DONNEES AVEC UNE CLE
Data processing with a key
DATA PROCESSING WITH A KEY
TRAITEMENT DE DONNEES AVEC UNE CLE
Local Applications (No Type Date): WO 2001FR1942 A 20010620; FR 20007887
A 20000620; AU 200169215 A 20010620; EP 2001947556 A 20010620; WO
2001FR1942 A 20010620; WO 2001FR1942 A 20010620; US 2002311693 A 20021219; CN 2001811332 A 20010620
Priority Applications (no., kind, date): FR 20007887 A 20000620

18/AN,AZ,TI/7 (Item 7 from file: 350)

0010908148
Digital signature calculation system for securing program codes, obtains
digital signature for signature target data from calculated partial

signatures, using secret key of program code owner

Original Titles:
SIGNATURE COMPUTING SYSTEM BY MOBILE AGENT AND RECORDING MEDIUM WITH PROGRAM RECORDED THEREON
Signature calculation system by use of mobile agent
Signature calculation system by use of mobile agent
Local Applications (No Type Date): US 2001760805 A 20010117; JP 20009037
A 20000118; JP 20009037 A 20000118; US 2001760805 A 20010117
Priority Applications (no., kind, date): JP 20009037 A 20000118; US 2001760805 A 20010117

18/AN,AZ,TI/8 (Item 8 from file: 350)

0010908052
Common key generation for cryptographic communication system, involves adding domain name of e-mail address of one entity to other entity e-mail
address if domain name is not included in e-mail address of one entity

Original Titles:
COMMON KEY GENERATING METHOD, COMMON KEY GENERATOR, **CIPHER** COMMUNICATION
METHOD, **CIPHER** COMMUNICATION SYSTEM AND RECORDING MEDIUM STORING PROGRAM
A common key production|generation device, an encryption communication method, an encryption communication system, and recording media
Common key generating method, common key generator, cryptographic communication method and cryptographic communication system
Local Applications (No Type Date): US 2001766807 A 20010122; JP 200016362
A 20000125; JP 200016362 A 20000125
Priority Applications (no., kind, date): JP 200016362 A 20000125

18/AN,AZ,TI/9 (Item 9 from file: 350)

0010801447
Public key certificate revoking method for electronic commerce, involves
ceasing publication of valid periodic freshness indicator, updates for public key certificate

Original Titles:
Blocked tree authorization and status systems
BLOCKED TREE AUTHORIZATION AND STATUS SYSTEMS
SYSTEMES D'AUTORISATION ET DE STATUT A ARBRE BLOQUE
Local Applications (No Type Date): WO 2000US21187 A 20000804; AU 200066200 A 20000804; US 1999147696 P 19990806; US 1999149315 P 19990817; US 1999154088 P 19990915; US 1999168002 P 19991130; US 1999169377 P 19991207; US 2000633149 A 20000804; US 2004949712 A

20040924
Priority Applications (no., kind, date): US 2004949712 A 20040924; US 2000633149 A 20000804; US 1999168002 P 19991130; US 1999154088 P 19990915; US 1999149315 P 19990817; US 1999147696 P 19990806; US 1999169377 P 19991207

18/AN,AZ,TI/10 (Item 10 from file: 350)

0010766720
Generation method for shared secret value between entities, involves computing common shared key for each entity by combining group short term public key, intra-entity shared key, and entity long term key

Original Titles:
SCHLUSSELAUSTAUSCHPROTOKOLL MIT AUFGETEILTEN SCHLUSSELN
SPLIT-KEY KEY-AGREEMENT PROTOCOL
PROTOCOLE D'ACCORD DE CLE CLE FRACTIONNEE
SCHLUSSELAUSTAUSCHPROTOKOLL MIT AUFGETEILTEN SCHLUSSELN
SPLIT-KEY KEY-AGREEMENT PROTOCOL
PROTOCOLE D'ACCORD DE CLE CLE FRACTIONNEE
Split-key key-agreement protocol
Split-key key-agreement protocol
SPLIT-KEY KEY-AGREEMENT PROTOCOL
PROTOCOLE D'ACCORD DE CLE CLE FRACTIONNEE
Local Applications (No Type Date): WO 2000CA838 A 20000719; AU 200061437 A 20000719; CA 2277633 A 19990719; EP 2000947716 A 20000719; WO 2000CA838 A 20000719; EP 2000947716 A 20000719; WO 2000CA838 A 20000719; DE 60006147 A 20000719; EP 2000947716 A 20000719; WO 2000CA838 A 20000719; US 2000619633 A 20000719; US 2000619633 A 20000719; US 2005155899 A 20050620
Priority Applications (no., kind, date): CA 2277633 A 19990719

18/AN,AZ,TI/11 (Item 11 from file: 350)

0010545988
Controlling and distributing information published using certification information and encryption for e.g. postage proof of payment system

Original Titles:
Verfahren zur Veroffentlichung von Zertifikationsinformationen, die eine wahlbare Untereinheit von Rechten darstellen, sowie Vorrichtung und tragbares Speichermedium zur Durchfuhrung **des** Verfahrens
Method for publishing certification information representative of selectable subsets of rights and apparatus and portable data storage media used to practice said method
Procede pour publier **des** informations de certification representant **des**

sous-ensembles **des** droits selectionnables et dispositif et support de donnees portatif pour executer ce procede
Method for publishing certification information representative of selectable subsets of rights and apparatus and portable data storage media
used to practice said method
Local Applications (No Type Date): EP 2000106075 A 20000330; CA 2303450
A 20000330; US 1999280529 A 19990330; CA 2303450 A 20000330
Priority Applications (no., kind, date): US 1999280529 A 19990330

18/AN,AZ,TI/12 (Item 12 from file: 350)

0010358324
Controlling and distributing information published using certification information and encryption for e.g. postage proof of payment system

Original Titles:
Verfahren zur Veroffentlichung von Zertifikationsinformationen, die von einer Vielzahl von Bevollmachtigten zertifiziert sind, sowie Vorrichtung
und tragbares Speichermedium zur Durchfuhrung **des** Verfahrens
Method for publishing certification information certified by a plurality of
authorities and apparatus and portable data storage media used to practice
said method
Procede pour publier **des** informations de certifications authentifie par
une pluralite d'autorites et dispositif et support de donnees portatif pour
executer ce procede
Method for publishing certification information certified by a plurality of
authorities and apparatus and portable data storage media used to practice
said method
Local Applications (No Type Date): EP 2000106074 A 20000330; CA 2303475
A 20000330; US 1999280527 A 19990330; CA 2303475 A 20000330
Priority Applications (no., kind, date): US 1999280527 A 19990330

18/AN,AZ,TI/13 (Item 13 from file: 350)

0009666487
Public key generating method for secure digital communication system

Original Titles:
Verfahren zur Erzeugung eines A(para)ffentlichen SchlA1/4ssels in einem sicheren digitalen Kommunikationssystem und implizites Zertifikat
IMPLIZITE ZERTIFIKATE
IMPLICIT CERTIFICATE SCHEME
SYSTEME DE CERTIFICATS IMPLICITES

Verfahren zur Erzeugung eines offentlichen Schlussels in einem sicheren digitalen Kommunikationssystem und implizites Zertifikat
Method of generating a public key in a secure digital communication system
and implicit certificate
Procede de generation d'une cle publique dans un systeme de communication
numerique et certificat implicite
Implicit certificate scheme
Implicit certificate scheme
IMPLICIT CERTIFICATE SCHEME
SYSTEME DE CERTIFICATS IMPLICITES
Local Applications (No Type Date): WO 1999CA244 A 19990323; CA 2232936 A
19980323; CA 2235359 A 19980420; AU 199928235 A 19990323; EP 1999908723 A 19990323; WO 1999CA244 A 19990323; JP 2000538463 A 19990323; AU 199928235 A 19990323; EP 1999908723 A 19990323; WO 1999CA244 A 19990323; DE 69918818 A 19990323; EP 1999908723 A 19990323; WO 1999CA244 A 19990323; WO 1999CA244 A 19990323; US 2000667819 A 20000922; WO 1999CA244 A 19990323; US 2000667817 A 20000922; US 2004921870 A 20040820; DE 69918818 A 19990323; EP 1999908723 A 19990323; WO 1999CA244 A 19990323; IL 138660 A 19990323
Priority Applications (no., kind, date): CA 2232936 A 19980323; CA 2235359 A 19980420

18/AN,AZ,TI/14 (Item 14 from file: 350)
DIALOG(R)File 350:(c) 2007 The Thomson Corporation. All rts. reserv.

0008956020
**Encrypted data recovery using split storage key system - using data key recovery response for partially decrypting data key encrypted by public key
of user and contained in enveloped data using split secret keys of key storage**

Original Titles:
Verfahren zur Rueckgewinnung verschluesselter Daten unter Verwendung eines
aufgeteilten Schluessels und zugehoerige Vorrichtung
Encrypted data recovery method using split storage key and system thereof
Procede de recuperation de donneeschiffrees utilisant une cle de stockage
fractionnee et systeme correspondant
CIPHER DATA RESTORATION METHOD, KEY REGISTRATION SYSTEM AND DATA RESTORATION SYSTEM
Encrypted data recovery method using split storage key and system thereof.
Local Applications (No Type Date): EP 1998302438 A 19980330; JP 199780081
A 19970331; US 199850066 A 19980330; JP 199780081 A 19970331
Priority Applications (no., kind, date): JP 199780081 A 19970331

18/AN,AZ,TI/15 (Item 15 from file: 350)

0008451619
**Electronic module for secure transactions, digital signatures & money transfers - I/O circuitry & maths coprocessor are coupled to DP circuit,
microprocessor to I/O circuitry, memory circuitry to microprocessor, module
is programmable to provide secure, encrypted data transfers between module
& DP circuitry**

Original Titles:
Verfahren, Vorrichtung, System und Firmware fur gesicherte Transaktionen
Method, apparatus, system and firmware for secure transactions
Procede, appareil, systeme et microprogrammation permettant d'effectuer **des** transactions sures
VERFAHREN,VORRICHTUNG,SYSTEM UND FIRMWARE FUR GESICHERTE TRANSAKTIONEN
METHOD, APPARATUS, SYSTEM AND FIRMWARE FOR SECURE TRANSACTIONS
PROCEDE, APPAREIL, SYSTEME ET MICROPROGRAMMATION PERMETTANT D'EFFECTUER **DES** TRANSACTIONS SURES
Method, apparatus, system and firmware for secure transactions.
Method, apparatus, and system for transferring units of value.
Method, apparatus, system and firmware for secure transactions.
Apparatus for transfer of secure information between a data carrying module
and an electronic device.
METHOD, APPARATUS, SYSTEM AND FIRMWARE FOR SECURE TRANSACTIONS
Local Applications (No Type Date): WO 1996US15471 A 19960926; AU 199673745 A 19960926; US 19954510 P 19950929; US 1996594983 A 19960131; EP 1996935993 A 19960926; WO 1996US15471 A 19960926; US 19954510 P 19950929; US 1996595014 A 19960131; CN 1996197307 A 19960926; AU 199673745 A 19960926; WO 1996US15471 A 19960926; JP 1997513652 A 19960926; MX 19982375 A 19980326; EP 1996935993 A 19960926; EP 2000109707 A 19960926; US 19954510 P 19950929; US 1996594983 A 19960131; US 199841190 A 19980310; WO 1996US15471 A 19960926; KR 1998702358 A 19980330; IL 123851 A 19960926; US 19954510
P 19950929; US 1996595014 A 19960131; US 19983541 A 19980106; WO 1996US15471 A 19960926; MX 19982375 A 19980326
Priority Applications (no., kind, date): US 199841190 A 19980310; US 19983541 A 19980106; WO 1996US15471 A 19960926; US 1996595014 A 19960131; US 19954510 P 19950929; US 1996594983 A 19960131

18/AN,AZ,TI/16 (Item 16 from file: 350)

0007855743
**Plain text block encryption in scalable key agile cryptography - pre-computes pseudorandom vectors used to encrypt text block, generates new
block of keystream as part of encryption process generating new vector**

Original Titles:
VERFAHREN UND EINRICHTUNG ZUR SCHNELLEN BLOCKCHIFFRIERUNG VON PAKETDATEN
METHOD AND APPARATUS FOR HIGH SPEED BLOCK CIPHERING OF PACKET DATA
PROCEDE ET SYSTEME DE CHIFFREMENT BLOC RAPIDE DE DONNEES EN PAQUETS
Scalable key agile cryptography.
METHOD AND APPARATUS FOR HIGH SPEED BLOCK CIPHERING OF PACKET DATA
Local Applications (No Type Date): WO 1996US5083 A 19960412; AU 199655428
A 19960412; EP 1996912718 A 19960412; WO 1996US5083 A 19960412; US
1995423082 A 19950417; US 1995518617 A 19950823; US 1995521056 A
19950829; JP 1996531817 A 19960412; WO 1996US5083 A 19960412
Priority Applications (no., kind, date): US 1995518617 A 19950823; US
1995423082 A 19950417; US 1995521056 A 19950829

18/AN,AZ,TI/17 (Item 17 from file: 350)

0003980166
Electronic transaction system for commercial computer documents - checks
sender-receiver, adds content certification function and double checks person by possession of secret key

Original Titles:
Elektronisches Transaktionssystem
Electronic transaction system
Systeme de transaction electronique
Methode und System fuer elektronische Transaktionen
Electronic transaction method and system
Methode et systeme de transaction electronique
ELECTRONIC TRANSACTION SYSTEM
Local Applications (No Type Date): EP 1986112177 A 19860903; JP 1985193735 A 19850904; JP 198696705 A 19860428; EP 1986112177 A 19860903; DE 3687934 A 19860903; EP 1986112177 A 19860903
Priority Applications (no., kind, date): JP 1985193735 A 19850904; JP 198696705 A 19860428

~~Full text patent files

```
? show files;ds
File 348:EUROPEAN PATENTS 1978-2007/ 200734
         (c) 2007 European Patent Office
File 349:PCT FULLTEXT 1979-2007/UB=20070823UT=20070816
         (c) 2007 WIPO/Thomson

Set     Items   Description
S1       8795   (KEY OR KEY- OR VARIABLE()VALUE OR
PASSWORD)()(INFORMATION
             OR DATA)
S2       8689   GENERAT??? OR AUTOGENERAT??? OR CONFIGUR? OR
CONSTRUCT??? -
```

```
             OR CREAT??? OR DERIV??? OR EXTRACT??? OR FORM??? OR
FORMULAT?-
             ?? OR MADE OR MAKE OR PRODUCE OR PRODUCING OR SYNTHESI?
S3       8795   (KEY OR KEY- OR VARIABLE()VALUE OR
PASSWORD)()(INFORMATION
             OR DATA)
S4       6492   SUM OR SUMMING OR COMBIN??? OR ADD OR ADDING
S5       2244   (INTERNAL OR PRIVATE OR SECRET OR RESTRICTED OR
LIMITED()A-
             CCESS)()((KEY OR KEYS OR VARIABLE()VALUE OR PASSWORD))
S6       1722   (UNIQUE OR DISTINCTIVE OR INDIVIDUAL OR
DISTINGUISHING)()(-
             ID OR IDENTIFIER OR IDENTIFIERS OR TOKEN OR TOKENS OR TAG
OR -
             TAGS OR INDICATOR OR INDICATORS) OR UI OR UID
S7       5491   DATA()DEVICE OR STORAGE()MEDIUM OR DISK OR DISKS OR
DISC OR
              DISCS OR CD OR DVD OR CDROM OR REMOVABLE()MEMORY OR
(THUMB OR
              USB OR FIREWIRE OR FLASH OR DETACHABLE OR REMOVABLE OR
PORTA-
             BLE OR MEMORY)()(DRIVE OR DRIVES)
S8       6887   ENCRYPTION()(ALGORITHM  OR FORMULA? ?) OR CIPHER OR DES
OR
             HASH OR MD5 OR AES OR SHA-1 OR SHA()1 OR SHA1 OR HMAC
S9       1974   S2(5N)S3
S10       185   S4(10N)(S5 OR (S6(5N)S7))
S11        11   S8(S)S9(S)S10
S12      2647   S2(10N)S3
S13       261   S4(20N)(S5 OR (S6(10N)S7))
S14        16   S8(S)S12(S)S13
S15         3   S14 AND IC=(H04K OR H04L)
S16        18   S11 OR S14 OR S15
S17        18   IDPAT (sorted in duplicate/non-duplicate order)
S18        17   IDPAT (primary/non-duplicate records only)
```

18/AN,AZ,TI/1 (Item 1 from file: 348)

02214709

Optical disk, method of manufacturing an optical disk and a reproduction apparatus

Optische Platte, Verfahren zur Herstellung einer optischen Platte und ein Wiedergabegerat

Disque optique, methode de fabrication d'un disque optique et un appareil de reproduction

APPLICATION (CC, No, Date): EP 2006027091 951116;
PRIORITY (CC, No, Date): JP 94283415 941117; JP 9516153 950202; JP 95261247 951009

18/AN,AZ,TI/2 (Item 2 from file: 348)

02059858
Systems and methods for secure transaction management and electronic rights
protection
System und Verfahren fur sichere Transaktionsverwaltung und elektronischen
Rechteschutz
Systemes et procedes de gestion de transactions securisees et de protection
des droits electroniques
APPLICATION (CC, No, Date): EP 2006075503 960213;
PRIORITY (CC, No, Date): US 388107 950213

18/AN,AZ,TI/3 (Item 3 from file: 348)
DIALOG(R)File 348:(c) 2007 European Patent Office. All rts. reserv.

02038564
Secure transaction management
Sicheres Transaktionsmanagement
Gestion de transactions securisees
APPLICATION (CC, No, Date): EP 2005077923 960213;
PRIORITY (CC, No, Date): US 388107 950213

18/AN,AZ,TI/4 (Item 4 from file: 348)
DIALOG(R)File 348:(c) 2007 European Patent Office. All rts. reserv.

01977623
Method and system for protecting individual information
Verfahren und System zum Schutz von individuellen Informationen
Procede et systeme pour protection d'informations individuelles
APPLICATION (CC, No, Date): EP 2005009353 050428;
PRIORITY (CC, No, Date): JP 2004136419 040430

18/AN,AZ,TI/5 (Item 5 from file: 348)
DIALOG(R)File 348:(c) 2007 European Patent Office. All rts. reserv.

01888484
Systems and methods for secure transaction management and electronic rights
protection
Systeme und Verfahren zur gesicherten Transaktionsverwaltung und
elektronischem Rechtsschutz
Systemes et procedes de gestion de transactions securisees et de protection
de droits electroniques
APPLICATION (CC, No, Date): EP 2004078254 960213;
PRIORITY (CC, No, Date): US 388107 950213

18/AN,AZ,TI/6 (Item 6 from file: 348)
DIALOG(R)File 348:(c) 2007 European Patent Office. All rts. reserv.

01869029
Systems and methods for secure transaction management and electronic rights
protection
Systeme und Verfahren zur gesicherten Transaktionsverwaltung und
elektronischem Rechtsschutz
Systemes et procedes de gestion de transactions securisees et de protection
de droits electroniques
APPLICATION (CC, No, Date): EP 2004078194 960213;
PRIORITY (CC, No, Date): US 388107 950213

18/AN,AZ,TI/7 (Item 7 from file: 348)
DIALOG(R)File 348:(c) 2007 European Patent Office. All rts. reserv.

01815760
Optical disk, method of manufacturing an optical disk and a reproduction
apparatus
Optische Platte, Verfahren zur Herstellung einer optischen Platte und
Wiedergabegerat
Disque optique, methode de fabrication d'un disque optique et methode de
reproduction
APPLICATION (CC, No, Date): EP 2004020082 951116;
PRIORITY (CC, No, Date): JP 94283415 941117; JP 9516153 950202; JP 95261247
951009

18/AN,AZ,TI/8 (Item 8 from file: 348)
DIALOG(R)File 348:(c) 2007 European Patent Office. All rts. reserv.

01752676
Systems and methods for secure transaction management and electronic rights
protection
Systeme und Verfahren zur gesicherten Transaktionsverwaltung und
elektronischem Rechtsschutz
Systemes et procedes de gestion de transactions securisees et de protection
de droits electroniques
APPLICATION (CC, No, Date): EP 2004075701 960213;
PRIORITY (CC, No, Date): US 388107 950213

18/AN,AZ,TI/9 (Item 9 from file: 348)
DIALOG(R)File 348:(c) 2007 European Patent Office. All rts. reserv.

01310513
Optical disk with copy protection, method for manufacturing and method for
reading such a disk

Optische Platte, Verfahren zur Herstellung und Verfahren zum Lesen einer
solchen Platte
Disque optique, procede pour fabriquer et proceder pour lire un tel disque
APPLICATION (CC, No, Date): EP 2001108949 951116;
PRIORITY (CC, No, Date): JP 94283415 941117; JP 9516153 950202; JP 95261247
951009

18/AN,AZ,TI/10 (Item 10 from file: 348)
DIALOG(R)File 348:(c) 2007 European Patent Office. All rts. reserv.

00779891
MARKING GENERATING APPARATUS, METHOD OF FORMING LASER MARKING ON OPTICAL
DISK, REPRODUCING APPARATUS, OPTICAL DISK AND OPTICAL DISK PRODUCING
METHOD
GERAT ZUR ERZEUGUNG EINER MARKIERUNG, VERFAHREN ZUR ERZEUGUNG EINER
LASERMARKIERUNG AUF EINER OPTISCHEN PLATTE, OPTISCHE PLATTE UND
VERFAHREN ZU DEREN HERSTELLUNG
APPAREIL GENERATEUR DE MARQUAGE, PROCEDE DE FORMATION D'UN MARQUAGE AU
LASER SUR DISQUE OPTIQUE, APPAREIL DE REPRODUCTION, DISQUE OPTIQUE ET
PROCEDE DE PRODUCTION DE DISQUE OPTIQUE
APPLICATION (CC, No, Date): EP 95938017 951116; WO 95JP2339 951116
PRIORITY (CC, No, Date): JP 94283415 941117; JP 9516153 950202; JP 95261247
951009

18/AN,AZ,TI/11 (Item 11 from file: 348)
DIALOG(R)File 348:(c) 2007 European Patent Office. All rts. reserv.

00641946
A METHOD AND APPARATUS FOR GENERATING A CIPHER STREAM
VERFAHREN UND EINRICHTUNG ZUR ERZEUGUNG EINER CHIFFRIERSEQUENZ
PROCEDE ET APPAREIL POUR GENERER UNE SUITE DE DONNEES CHIFFREE
APPLICATION (CC, No, Date): EP 94903705 931230; WO 93AU687 931230
PRIORITY (CC, No, Date): AU 92PL6577 921230

18/AN,AZ,TI/12 (Item 12 from file: 349)
DIALOG(R)File 349:(c) 2007 WIPO/Thomson. All rts. reserv.

01129704
DEAD NOZZLE COMPENSATION
COMPENSATION D'UNE BUSE HORS ETAT DE FONCTIONNEMENT
Application: WO 2003AU1616 20031202 (PCT/WO AU03001616)

18/AN,AZ,TI/13 (Item 13 from file: 349)

DIALOG(R)File 349:(c) 2007 WIPO/Thomson. All rts. reserv.

00989323
A SECURE ACCESS METHOD AND SYSTEM
PROCEDE ET SYSTEME D'ACCES SECURISE
Application: WO 2002US27303 20020826 (PCT/WO US0227303)

18/AN,AZ,TI/14 (Item 14 from file: 349)
DIALOG(R)File 349:(c) 2007 WIPO/Thomson. All rts. reserv.

00984069
PRINTING CARTRIDGE WITH AN INTEGRATED CIRCUIT DEVICE
CARTOUCHE D'IMPRESSION A DISPOSITIF A CIRCUIT INTEGRE
Application: WO 2002AU914 20020709 (PCT/WO AU0200914)

18/AN,AZ,TI/15 (Item 15 from file: 349)
DIALOG(R)File 349:(c) 2007 WIPO/Thomson. All rts. reserv.

00984066
A PRINTING CARTRIDGE WITH CAPACITIVE SENSOR IDENTIFICATION
CARTOUCHE D'IMPRESSION COMPORTANT UNE FONCTION D'IDENTIFICATION DES
CAPTEURS CAPACITIFS
Application: WO 2002AU1055 20020806 (PCT/WO AU0201055)

18/AN,AZ,TI/16 (Item 16 from file: 349)
DIALOG(R)File 349:(c) 2007 WIPO/Thomson. All rts. reserv.

00483529
CRYPTOGRAPHIC CO-PROCESSOR
COPROCESSEUR CRYPTOGRAPHIQUE
Application: WO 98US19316 19980916 (PCT/WO US9819316)

18/AN,AZ,TI/17 (Item 17 from file: 349)
DIALOG(R)File 349:(c) 2007 WIPO/Thomson. All rts. reserv.

00344642
SYSTEMS AND METHODS FOR SECURE TRANSACTION MANAGEMENT AND ELECTRONIC RIGHTS
PROTECTION
SYSTEMES ET PROCEDES DE GESTION SECURISEE DE TRANSACTIONS ET DE PROTECTION
ELECTRONIQUE DES DROITS
Application: WO 96US2303 19960213 (PCT/WO US9602303)

~~Bibliographic NPL files

? show files;ds
File 2:INSPEC 1898-2007/Aug W4
(c) 2007 Institution of Electrical Engineers
File 35:Dissertation Abs Online 1861-2007/Jul
(c) 2007 ProQuest Info&Learning

```
File  65:Inside Conferences 1993-2007/Sep 04
         (c) 2007 BLDSC all rts. reserv.
File  99:Wilson Appl. Sci & Tech Abs 1983-2007/Jul
         (c) 2007 The HW Wilson Co.
File 474:New York Times Abs 1969-2007/Aug 31
         (c) 2007 The New York Times
File 475:Wall Street Journal Abs 1973-2007/Sep 01
         (c) 2007 The New York Times
File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
         (c) 2002 The Gale Group
File 256:TecInfoSource 82-2007/Feb
         (c) 2007 Info.Sources Inc
File 169:Insurance Periodicals 1984-1999/Nov 15
         (c) 1999 NILS Publishing Co.

Set     Items   Description
S1       1480   (KEY OR KEY- OR VARIABLE()VALUE OR
PASSWORD)()(INFORMATION
             OR DATA)
S2        728   GENERAT??? OR AUTOGENERAT??? OR CONFIGUR? OR
CONSTRUCT??? -
             OR CREAT??? OR DERIV??? OR EXTRACT??? OR FORM??? OR
FORMULAT?-
             ?? OR MADE OR MAKE OR PRODUCE OR PRODUCING OR SYNTHESI?
S3       1480   (KEY OR KEY- OR VARIABLE()VALUE OR
PASSWORD)()(INFORMATION
             OR DATA)
S4         95   SUM OR SUMMING OR COMBIN??? OR ADD OR ADDING
S5         29   (INTERNAL OR PRIVATE OR SECRET OR RESTRICTED OR
LIMITED()A-
             CCESS)()((KEY OR KEYS OR VARIABLE()VALUE OR PASSWORD))
S6          1   (UNIQUE OR DISTINCTIVE OR INDIVIDUAL OR
DISTINGUISHING)()(-
             ID OR IDENTIFIER OR IDENTIFIERS OR TOKEN OR TOKENS OR TAG
OR -
             TAGS OR INDICATOR OR INDICATORS) OR UI OR UID
S7         37   DATA()DEVICE OR STORAGE()MEDIUM OR DISK OR DISKS OR
DISC OR
              DISCS OR CD OR DVD OR CDROM OR REMOVABLE()MEMORY OR
(THUMB OR
              USB OR FIREWIRE OR FLASH OR DETACHABLE OR REMOVABLE OR
PORTA-
             BLE OR MEMORY)()(DRIVE OR DRIVES)
S8         19   ENCRYPTION()(ALGORITHM  OR FORMULA? ?) OR CIPHER OR DES
OR
             HASH OR MD5 OR AES OR SHA-1 OR SHA()1 OR SHA1 OR HMAC
S9        130   S2(5N)S3
S10         0   S4(10N)(S5 OR (S6(5N)S7))
S11         0   S8(S)S9(S)S10
S12       207   S2(10N)S3
S13         0   S4(20N)(S5 OR (S6(10N)S7))
S14         0   S2 AND S3 AND S4 AND (S5 OR (S6 AND S7)) AND S8
S15         2   S4 AND (S5 OR (S6 AND S7))
S16        29   S5 OR (S6 AND S7)
S17        13   S16 AND (S2 OR S7 OR S8)
S18        15   S15 OR S17
S19         7   S18 NOT PY>1999
```

S20 7 S19 NOT PD=19990210:20071031
S21 7 RD (unique items)

21/6/1 (Item 1 from file: 2)
07624005 INSPEC Abstract Number: B2000-08-6120D-001, C2000-08-6130S-001
Title: Implementation of private key **data encription using gate arrays**
Publication Date: Dec. 1999
Copyright 2000, IEE

21/6/2 (Item 2 from file: 2)
06768051 INSPEC Abstract Number: B9801-6120B-045, C9801-6130S-033
Title: Cryptographic key recovery
Publication Date: 1997
Copyright 1997, IEE

21/6/3 (Item 3 from file: 2)
06589249 INSPEC Abstract Number: B9707-6120B-011, C9707-6130S-011
Title: Linking information reconciliation and privacy amplification
Publication Date: Spring 1997
Copyright 1997, IEE

21/6/4 (Item 4 from file: 2)
06496176 INSPEC Abstract Number: B9703-6120B-118, C9703-6130S-056
Title: Non-repudiation without public-key
Publication Date: 1996
Copyright 1997, IEE

21/6/5 (Item 5 from file: 2)
06212845 INSPEC Abstract Number: B9604-6120B-122, C9604-6130S-064
Title: Foiling active network impersonation attacks made **in collusion with an insider**
Publication Date: 1996
Copyright 1996, IEE

21/6/6 (Item 6 from file: 2)
04472553 INSPEC Abstract Number: B89063123, C89061067
Title: Information theory of shift register sequences
Publication Date: 1989

21/6/7 (Item 1 from file: 35)
01164497 ORDER NO: AAD91-19534
ON THE KEY INFORMATION REDUNDANCY IN SECRET - KEY **CRYPTOSYSTEMS (CRYPTOSYSTEMS,** CIPHER **SYSTEMS)**
Year: 1990

~~Full text NPL files - 1

```
? show files;ds
File  20:Dialog Global Reporter 1997-2007/Sep 04
         (c) 2007 Dialog

Set     Items   Description
S1      58938   (KEY OR KEY- OR VARIABLE()VALUE OR
PASSWORD)()(INFORMATION
             OR DATA)
S2      54343   GENERAT??? OR AUTOGENERAT??? OR CONFIGUR? OR
CONSTRUCT??? -
             OR CREAT??? OR DERIV??? OR EXTRACT??? OR FORM??? OR
FORMULAT?-
             ?? OR MADE OR MAKE OR PRODUCE OR PRODUCING OR SYNTHESI?
S3      58938   (KEY OR KEY- OR VARIABLE()VALUE OR
PASSWORD)()(INFORMATION
             OR DATA)
S4      27975   SUM OR SUMMING OR COMBIN??? OR ADD OR ADDING
S5         51   (INTERNAL OR PRIVATE OR SECRET OR RESTRICTED OR
LIMITED()A-
             CCESS)()((KEY OR KEYS OR VARIABLE()VALUE OR PASSWORD))
S6         52   (UNIQUE OR DISTINCTIVE OR INDIVIDUAL OR
DISTINGUISHING)()(-
             ID OR IDENTIFIER OR IDENTIFIERS OR TOKEN OR TOKENS OR TAG
OR -
             TAGS OR INDICATOR OR INDICATORS) OR UI OR UID
S7       2768   DATA()DEVICE OR STORAGE()MEDIUM OR DISK OR DISKS OR
DISC OR
              DISCS OR CD OR DVD OR CDROM OR REMOVABLE()MEMORY OR
(THUMB OR
              USB OR FIREWIRE OR FLASH OR DETACHABLE OR REMOVABLE OR
PORTA-
             BLE OR MEMORY)()(DRIVE OR DRIVES)
S8        477   ENCRYPTION()(ALGORITHM  OR FORMULA? ?) OR CIPHER OR DES
OR
             HASH OR MD5 OR AES OR SHA-1 OR SHA()1 OR SHA1 OR HMAC
S9       1068   S2(5N)S3
S10         1   S4(10N)(S5 OR (S6(5N)S7))
S11         0   S8(S)S9(S)S10
S12      2331   S2(10N)S3
S13         2   S4(20N)(S5 OR (S6(10N)S7))
S14         0   S8(S)S12(S)S13
S15         0   S2(S)S3(S)S4(S)(S5 OR (S6(S)S7))(S)S8
S16        56   S5 OR (S6 AND S7)
S17        45   S16(S)(S2 OR S3 OR S4 OR S8)
S18         7   S17 NOT PY>1999
S19         5   RD  (unique items)

 19/6/1
08772628  (USE FORMAT 7 OR 9 FOR FULLTEXT)
Deutsche Selects Two Firms' E-Commerce Software
October 20, 1999
WORD COUNT:  437


 19/6/2
07479223  (USE FORMAT 7 OR 9 FOR FULLTEXT)
Sonera,  Gemplus  and EDS Launch Global Initiative To Promote Secure
```

Mobile
Commerce
September 28, 1999
WORD COUNT: 1269

19/6/3
05041216 (USE FORMAT 7 OR 9 FOR FULLTEXT)
Carroll-Net Selects Intelispan's VPN Service
April 21, 1999
WORD COUNT: 727

19/6/4
04569976 (USE FORMAT 7 OR 9 FOR FULLTEXT)
SunStar Communications Selects Intelispan for VPN and Dedicated Internet
Services
March 09, 1999
WORD COUNT: 624

19/6/5
04044073 (USE FORMAT 7 OR 9 FOR FULLTEXT)
Pollard, Compaq, Gilmore Win 1999 RSA Award
January 18, 1999
WORD COUNT: 1073

~~Full text NPL - 2

```
? show files;ds
File   9:Business & Industry(R) Jul/1994-2007/Aug 28
         (c) 2007  The Gale Group
File  15:ABI/Inform(R) 1971-2007/Sep 03
         (c) 2007 ProQuest Info&Learning
File  16:Gale Group PROMT(R) 1990-2007/Aug 30
         (c) 2007 The Gale Group
File 148:Gale Group Trade & Industry DB 1976-2007/Aug 28
         (c)2007 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 275:Gale Group Computer DB(TM) 1983-2007/Jul 24
         (c) 2007 The Gale Group
File 476:Financial Times Fulltext 1982-2007/Sep 02
         (c) 2007 Financial Times Ltd
File 621:Gale Group New Prod.Annou.(R) 1985-2007/Aug 28
         (c) 2007 The Gale Group
File 624:McGraw-Hill Publications 1985-2007/Sep 04
         (c) 2007 McGraw-Hill Co. Inc
File 634:San Jose Mercury  Jun 1985-2007/Aug 30
         (c) 2007 San Jose Mercury News
File 636:Gale Group Newsletter DB(TM) 1987-2007/Aug 30
         (c) 2007 The Gale Group

Set     Items   Description
S1      42803   (KEY OR KEY- OR VARIABLE()VALUE OR
```

```
PASSWORD)()(INFORMATION
             OR DATA)
S2       32704   GENERAT??? OR AUTOGENERAT??? OR CONFIGUR? OR
CONSTRUCT??? -
             OR CREAT??? OR DERIV??? OR EXTRACT??? OR FORM??? OR
FORMULAT?-
             ?? OR MADE OR MAKE OR PRODUCE OR PRODUCING OR SYNTHESI?
S3       42803   (KEY OR KEY- OR VARIABLE()VALUE OR
PASSWORD)()(INFORMATION
             OR DATA)
S4       13061   SUM OR SUMMING OR COMBIN??? OR ADD OR ADDING
S5         314   (INTERNAL OR PRIVATE OR SECRET OR RESTRICTED OR
LIMITED()A-
             CCESS)()((KEY OR KEYS OR VARIABLE()VALUE OR PASSWORD))
S6         169   (UNIQUE OR DISTINCTIVE OR INDIVIDUAL OR
DISTINGUISHING)()(-
             ID OR IDENTIFIER OR IDENTIFIERS OR TOKEN OR TOKENS OR TAG
OR -
             TAGS OR INDICATOR OR INDICATORS) OR UI OR UID
S7        3900   DATA()DEVICE OR STORAGE()MEDIUM OR DISK OR DISKS OR
DISC OR
              DISCS OR CD OR DVD OR CDROM OR REMOVABLE()MEMORY OR
(THUMB OR
              USB OR FIREWIRE OR FLASH OR DETACHABLE OR REMOVABLE OR
PORTA-
             BLE OR MEMORY)()(DRIVE OR DRIVES)
S8         646   ENCRYPTION()(ALGORITHM  OR FORMULA? ?) OR CIPHER OR DES
OR
             HASH OR MD5 OR AES OR SHA-1 OR SHA()1 OR SHA1 OR HMAC
S9        2904   S2(5N)S3
S10          6   S4(10N)(S5 OR (S6(5N)S7))
S11          0   S8(S)S9(S)S10
S12       5267   S2(10N)S3
S13         11   S4(20N)(S5 OR (S6(10N)S7))
S14          0   S8(S)S12(S)S13
S15        352   S5 OR (S6 AND S7)
S16        278   S15(S)(S2 OR S3 OR S4 OR S8)
S17         42   S4(S)S15
S18         30   S17(S)(S2 OR S3 OR S8)
S19         33   S10 OR S18
S20         27   S19 NOT PY>1999
S21         19   S20 NOT PD=19990210:20071031
S22         14   RD  (unique items)

 22/6/1     (Item 1 from file: 9)
00864754  Supplier Number: 23399840     (USE FORMAT 7 OR 9 FOR FULLTEXT)
S-A UNVEILS SECURITY SYSTEM
January 15, 1996
WORD COUNT:  1146


 22/6/2     (Item 1 from file: 15)
01769006  04-19997
                  **USE FORMAT 7 OR 9 FOR FULL TEXT**
Encryption:  A 21st century national security dilemma
Jul 1998   LENGTH: 24 Pages
WORD COUNT: 12421
```

22/6/3 (Item 2 from file: 15)
01663108 03-14098
USE FORMAT 7 OR 9 FOR FULL TEXT
Protecting digital media content
Jul 1998 LENGTH: 10 Pages
WORD COUNT: 4301

22/6/4 (Item 3 from file: 15)
01271601 99-20997
USE FORMAT 7 OR 9 FOR FULL TEXT
Proposed IETF standard to ease a variety of remote access concerns
Aug 12, 1996 LENGTH: 1 Pages
WORD COUNT: 772

22/6/5 (Item 1 from file: 16)
05753303 Supplier Number: 50237197 (USE FORMAT 7 FOR FULLTEXT)
CYLINK SIGNS OFF ON US POSTAL CERTIFICATE AUTHORITY
August 13, 1998
Word Count: 870

22/6/6 (Item 2 from file: 16)
01747641 Supplier Number: 42189170 (USE FORMAT 7 FOR FULLTEXT)
ADDRESSING SECURITY
July, 1991
Word Count: 1555

22/6/7 (Item 1 from file: 148)
08472225 SUPPLIER NUMBER: 18006515 (USE FORMAT 7 OR 9 FOR FULL TEXT)
S-A unveils security system. (Scientific-Atlanta Inc.)
Jan 15, 1996
WORD COUNT: 1253 LINE COUNT: 00102

22/6/8 (Item 2 from file: 148)
04132346 SUPPLIER NUMBER: 07826888 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Lock up your data. (Software Review) (UltraLock and FastLock data security programs) (evaluation)
Oct 11, 1989
WORD COUNT: 1675 LINE COUNT: 00131

22/6/9 (Item 1 from file: 275)
02146244 SUPPLIER NUMBER: 20297029 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Lesson 115: IP security. (IETF's IP Security protocol suite) (Tutorial) (Technology Information)
Feb, 1998
WORD COUNT: 1950 LINE COUNT: 00153

22/6/10 (Item 2 from file: 275)
02128281 SUPPLIER NUMBER: 20086545 (USE FORMAT 7 OR 9 FOR FULL TEXT)
The true cost of doing business. (Microsoft's total-cost-of-ownership initiatives) (Company Business and Marketing)
Jan, 1998
WORD COUNT: 6029 LINE COUNT: 00478

22/6/11 (Item 3 from file: 275)
02074073 SUPPLIER NUMBER: 19516596 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Keep your notebook data secure with Session Key. (Secured Communications Canada Session Key PC Card security device) (Hardware Review) (Evaluation)
July, 1997
WORD COUNT: 530 LINE COUNT: 00044

22/6/12 (Item 4 from file: 275)
01915600 SUPPLIER NUMBER: 18109717 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Battening down the hatches. (securing dial-in remote access systems) (Technology Tutorial)
April, 1996
WORD COUNT: 3569 LINE COUNT: 00276

22/6/13 (Item 5 from file: 275)
01613921 SUPPLIER NUMBER: 13901763 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Tools and utilities. (software packages that help database developers prototype and design applications, query, and create help systems, among other uses) (1993 Database Buyer's Guide Special Issue) (Buyers Guide)
June 15, 1993
WORD COUNT: 45702 LINE COUNT: 03876

22/6/14 (Item 1 from file: 636)
01109969 Supplier Number: 40810254 (USE FORMAT 7 FOR FULLTEXT)
Research into secure transaction services
June, 1989
Word Count: 283

~~Full text NPL files - 3

? show files;ds
File 610:Business Wire 1999-2007/Sep 04
(c) 2007 Business Wire.
File 613:PR Newswire 1999-2007/Sep 04
(c) 2007 PR Newswire Association Inc

```
File 810:Business Wire 1986-1999/Feb 28
         (c) 1999 Business Wire
File 813:PR Newswire 1987-1999/Apr 30
         (c) 1999 PR Newswire Association Inc
File 239:Mathsci 1940-2007/Oct
         (c) 2007 American Mathematical Society
File 267:Finance & Banking Newsletters 2007/Aug 20
         (c) 2007 Dialog
File 268:Banking Info Source 1981-2007/Aug W2
         (c) 2007 ProQuest Info&Learning
File 553:Wilson Bus. Abs. 1982-2007/Aug
         (c) 2007 The HW Wilson Co
File 625:American Banker Publications 1981-2007/Aug 29
         (c) 2007 American Banker
File 626:Bond Buyer Full Text 1981-2007/Aug 30
         (c) 2007 Bond Buyer
File 647:CMP  Computer Fulltext 1988-2007/Sep W4
         (c) 2007 CMP Media, LLC
File 674:Computer News Fulltext 1989-2006/Sep W1
         (c) 2006 IDG Communications
File  13:BAMP 2007/Aug W4
         (c) 2007  The Gale Group
File  56:Computer and Information Systems Abstracts 1966-2007/Aug
         (c) 2007 CSA.
File  75:TGG Management Contents(R) 86-2007/Aug W4
         (c) 2007 The Gale Group
File 249:Mgt. & Mktg. Abs. 1976-2007Apr W5
         (c) 2007 Pira International

Set     Items   Description
S1      12671   (KEY OR KEY- OR VARIABLE()VALUE OR
PASSWORD)()(INFORMATION
             OR DATA)
S2      10136   GENERAT??? OR AUTOGENERAT??? OR CONFIGUR? OR
CONSTRUCT??? -
             OR CREAT??? OR DERIV??? OR EXTRACT??? OR FORM??? OR
FORMULAT?-
             ?? OR MADE OR MAKE OR PRODUCE OR PRODUCING OR SYNTHESI?
S3      12671   (KEY OR KEY- OR VARIABLE()VALUE OR
PASSWORD)()(INFORMATION
             OR DATA)
S4       3985   SUM OR SUMMING OR COMBIN??? OR ADD OR ADDING
S5         84   (INTERNAL OR PRIVATE OR SECRET OR RESTRICTED OR
LIMITED()A-
             CCESS)()((KEY OR KEYS OR VARIABLE()VALUE OR PASSWORD))
S6         38   (UNIQUE OR DISTINCTIVE OR INDIVIDUAL OR
DISTINGUISHING)()(-
             ID OR IDENTIFIER OR IDENTIFIERS OR TOKEN OR TOKENS OR TAG
OR -
             TAGS OR INDICATOR OR INDICATORS) OR UI OR UID
S7        964   DATA()DEVICE OR STORAGE()MEDIUM OR DISK OR DISKS OR
DISC OR
              DISCS OR CD OR DVD OR CDROM OR REMOVABLE()MEMORY OR
(THUMB OR
              USB OR FIREWIRE OR FLASH OR DETACHABLE OR REMOVABLE OR
PORTA-
             BLE OR MEMORY)()(DRIVE OR DRIVES)
```

```
S8         199   ENCRYPTION()(ALGORITHM  OR FORMULA? ?) OR CIPHER OR DES
OR
              HASH OR MD5 OR AES OR SHA-1 OR SHA()1 OR SHA1 OR HMAC
S9         946   S2(5N)S3
S10          3   S4(10N)(S5 OR (S6(5N)S7))
S11          0   S8(S)S9(S)S10
S12       1787   S2(10N)S3
S13          3   S4(20N)(S5 OR (S6(10N)S7))
S14          0   S8(S)S12(S)S13
S15         85   S5 OR (S6(S)S7)
S16         69   S15(S)(S2 OR S3 OR S4 OR S8)
S17         37   S16 NOT PY>1999
S18         28   S17 NOT PD=19990210:20071031
S19         26   RD  (unique items)
```

19/6/1 (Item 1 from file: 810)
0714335 BW1164

MYKOTRONX WESTERN DATACOM: Rainbow subsidiary Mykotronx and Western Datacom
announce joint development of industry's first dual-mode cryptographic
modem -- FORDESZA

June 17, 1997

19/6/2 (Item 2 from file: 810)
0665903 BW0231

SPYRUS MAC: Multi-Card Accelerator from SPYRUS is Hardware Cryptographic
Digital Signature Server Solution; Scaleable, High-Assurance
Certification Authority, Remote Access, and Other Digital Content
Signing Applications Now Enabled

January 27, 1997

19/6/3 (Item 3 from file: 810)
0520713 BW1046

ATALLA: Atalla Begins Shipping Hardware-Based Security for the Internet

October 02, 1995

19/6/4 (Item 1 from file: 813)
1405544 SFM052
Pollard, Compaq, Gilmore Win 1999 RSA Award

DATE: January 18, 1999
WORD COUNT: 1,090

19/6/5 (Item 2 from file: 813)
0990442 MNTU011
Network Systems Security Devices Tested by Department of Defense-Sponsored
'SPOCK' Program

DATE: September 3, 1996
WORD COUNT: 645

19/6/6 (Item 3 from file: 813)
0854260 NYFNS1
BACK TO SCHOOL, BUT NOT BACK TO BASICS; PERSONAL ELECTRONICS ARE TOPS ON
BACK TO SCHOOL LISTS

DATE: August 28, 1995
WORD COUNT: 498

19/6/7 (Item 4 from file: 813)
0781857 NE003
PERSONAL TOKEN APPLICATION IN MOBILE COMPUTING IS JUST THE BEGINNING

DATE: January 25, 1995
WORD COUNT: 1,419

19/6/8 (Item 5 from file: 813)
0776490 NY011
TELEQUIP CORPORATION INTRODUCES THE CRYPTA PLUS CARD

DATE: January 9, 1995
WORD COUNT: 790

19/6/9 (Item 1 from file: 268)
00327194 (USE FORMAT 7 OR 9 FOR FULLTEXT)
Stopping cyberthieves
Jan 1998
WORD COUNT: 02351

19/6/10 (Item 2 from file: 268)
00285781 (USE FORMAT 7 OR 9 FOR FULLTEXT)
Digital signatures: Time-saving technology at your fingertips
Apr 1996
WORD COUNT: 01495

19/6/11 (Item 1 from file: 625)
0190712
*** Mellon Starts Internet-Based Corporate Service**
November 13, 1996

19/6/12 (Item 2 from file: 625)

0183163
*** Banks Seeking Cheaper EDI on Internet**
June 6, 1996

19/6/13 (Item 1 from file: 647)
01142056 CMP ACCESSION NUMBER: INW19971020S0078
Breaking The Code For Network Security (Buyer's Guide)
PUBLICATION DATE: 971020
WORD COUNT: 434

19/6/14 (Item 2 from file: 647)
01097494 CMP ACCESSION NUMBER: NWC19960715S0021
Psstt! Security Designed For Your Eyes Only (Security)
PUBLICATION DATE: 960715
WORD COUNT: 1121

19/6/15 (Item 3 from file: 647)
01093295 CMP ACCESSION NUMBER: EET19960603S0043
Smart-card makers ramp up
PUBLICATION DATE: 960603
WORD COUNT: 1176

19/6/16 (Item 4 from file: 647)
01021798 CMP ACCESSION NUMBER: OST19940523S1526
Las Vegas Show Floor Reveals Product Trends
PUBLICATION DATE: 940523
WORD COUNT: 342

19/6/17 (Item 5 from file: 647)
00607536 CMP ACCESSION NUMBER: NWC19910701S2952
Network Security Seeking Security in the Enterprise-wide Network (Feature
1)
PUBLICATION DATE: 910701
WORD COUNT: 3374

19/6/18 (Item 1 from file: 674)
071829
Serious about Security? Who the X.509 are you?
Publication Date: February 01, 1999

19/6/19 (Item 2 from file: 674)
053733
Proposed IETF standard to ease a variety of remote access concerns
Protocol authenticates remote dial-up users and provides for secure connections.
Publication Date: August 12, 1996

19/6/20 (Item 3 from file: 674)
032271
Encryption restriction policy hurts users, vendors
Publication Date: August 23, 1993

19/6/21 (Item 4 from file: 674)
028435
RSA public-key encryption plan wins support
Publication Date: January 25, 1993

19/6/22 (Item 5 from file: 674)
017538
Security is key to ECON
Publication Date: August 19, 1991

19/6/23 (Item 1 from file: 13)
00517579 Supplier Number: 23688494 (USE FORMAT 7 OR 9 FOR FULLTEXT)
Is Encryption Policy Jumbled?
November 1996
WORD COUNT: 1109

19/6/24 (Item 2 from file: 13)
00505602 Supplier Number: 23623265 (USE FORMAT 7 OR 9 FOR FULLTEXT)
SOMETHING TO TALK ABOUT
September 1996
WORD COUNT: 3842

19/6/25 (Item 1 from file: 56)
0000555080 IP ACCESSION NO: 200610-90-131075
Network security under siege: the timing attack
PUBLICATION DATE: 1996

19/6/26 (Item 2 from file: 56)
0000294350 IP ACCESSION NO: 315050
Cryptographic key recovery
PUBLICATION DATE: 1997